NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EVALUATION AND IMPLEMENTATION OF MEDIA-INDEPENDENT HANDOVER IN HASTILY FORMED NETWORKS

by

Khaled Ferchichi

March 2013

Thesis Advisor: Geoffrey Xie
Co-Advisor: Brian Steckler

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 2013	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE EVALUATION AND IMPLEMENTATION OF MEDIA-INDEPENDENT HANDOVER IN HASTILY FORMED NETWORKS	5. FUNDING NUMBERS
6. AUTHOR(S) Khaled Ferchichi	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Hastily formed networks (HFNs) are deployed in the aftermath of a disaster. They are formed by people from different communities who work together in a shared conversation space. The network component of the shared conversation space is the backbone of the communication system. It can be created using technologies such as Ethernet, WiFi, and WiMAX. HFNs face huge challenges in the integration of mobile devices that will provide better mobility in the conversation space, especially with the fast proliferation of multimodal mobile devices that support many technologies. In this research we investigate if the integration of the Media Independent Handover (MIH) in HFNs can be an adequate solution for these problems.

MIH could be the solution to not only the mobility and roaming problems but also for other HFN problems due to the intelligent layer-two functions it offers. We tried to combine MIH and Session Initiation Protocol (SIP) protocol in order to provide HFN users with a better user experience especially during video and audio conversations. The research showed the limitations of MIH and its open source implementation (ODTONE). We were also able to describe the steps needed for the integration of SIP and MIH.

14. SUBJECT TERMS HFN, MIH, SIP, IEEE 802.21, wifi, seamless handover, ODTONE, Mobility	15. NUMBER OF PAGES 73
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EVALUATION AND IMPLEMENTATION OF MEDIA-INDEPENDENT HANDOVER IN HASTILY FORMED NETWORKS

Khaled Ferchichi
B.S., Tunisian Naval Academy, 2006
Lieutenant, Tunisian Navy

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2013

Author: Khaled Ferchichi

Approved by: Geoffrey Xie
Thesis Advisor

Brian Steckler
Thesis Co-Advisor

Dan Boger
Chair, Department of Information Sciences Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Hastily formed networks (HFNs) are deployed in the aftermath of a disaster. They are formed by people from different communities who work together in a shared conversation space. The network component of the shared conversation space is the backbone of the communication system. It can be created using technologies such as Ethernet, WiFi, and WiMAX. HFNs face huge challenges in the integration of mobile devices that will provide better mobility in the conversation space, especially with the fast proliferation of multimodal mobile devices that support many technologies. In this research we investigate if the integration of the Media Independent Handover (MIH) in HFNs can be an adequate solution for these problems.

MIH could be the solution to not only the mobility and roaming problems but also for other HFN problems due to the intelligent layer-two functions it offers. We tried to combine MIH and Session Initiation Protocol (SIP) protocol in order to provide HFN users with a better user experience especially during video and audio conversations. The research showed the limitations of MIH and its open source implementation (ODTONE). We were also able to describe the steps needed for the integration of SIP and MIH.

.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

MIIS Media Independent Information Service

VSAT Very Small Aperture Terminal

3G 3rd Generation

3GPP 3rd Generation Partnership Project

4G 4th Generation

AOR Area of Responsibility

AP Access Point

API Application Programming Interface

AS-SIP Assured Services Session Initiation Protocol

BS Base Station

CM Connection Manager

FMIPv6 Fast Mobile IPv6

FN foreign network

GSM Global System for Mobile Communication

HA/DR Human Assistance and disaster relief

HFN Hastily Formed Networks

HN Home Network

HTTP Hyper Text Transfer Protocol

IETF Internet Engineering Task Force

LLC Logical Link Control

LTE Long Term Evolution

MAC Medium Access Control

MICS Media Independent Command Service

MIES Media Independent Even Services

MIH Media Independent Handover

MIHF Media Independent Handover Function

MIHF Media Independent Handover Function

MIPv6 Mobile IPv6

MN Mobile Node

NIC Network Interface Card

NMM Network Mobility Manager

NOC Network Operation Center

ODTONE Open Dot Twenty ONE

OPMIPv6 Open Proxy Mobile IPv6

PMIPv6 Proxy Mobile IPv6

PoA Points of Attachment

PoS Points of Service

QoS Quality of Service

SAP Service Access Point

SATCOM Satellite Communication

SIP Session Initiation Protocol

UA User Agent

UAC User Agent Client

UAS User Agent Server

VoIP Voice Over IP

WG Working Group

WiMAX Worldwide Interoperability for Microwave Access

ACKNOWLEDGMENTS

This work could not be completed without the support of my family, especially my father, Belgacem, and my mother, Fatma. I would like to thank them for their prayers and their unlimited support.

I would like also to thank my thesis advisors Geoffrey Xie and Brian Steckler for their help, support and patience.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. INTRODUCTION

Hastily formed networks (HFNs), as defined by Denning (2006), are a "network of people, established rapidly from different communities, working together in a shared conversation space." The conversation space, especially the network layer, is the backbone of the communication system. It can be created—depending on the situation—using different technologies such as Ethernet, WiFi, and WiMAX. As we witness the fast proliferation of new mobile devices with multimodal connectivity capabilities (WiFi, 3G, Bluetooth) HFNs face huge challenges in integration of these devices and the exploitation of their capabilities of supporting heterogeneous network technologies at the same time. Roaming smoothly across different network technologies that form the conversation space may seem but a convenience for HA/DR early responders, but it will become a need as networks get complicated and overlap. To tackle these challenges and problems, we propose the integration and use of the Media Independent Handover (MIH), a standard defined by IEEE. MIH promises to allow mobile terminals to roam seamlessly between heterogeneous network technologies. Moreover, it promises an intelligent network selection without user intervention.

B. THE RESEARCH PROBLEM

1. Problem Statement

Hastily formed networks provide only restricted mobility to users inside the conversation space and between different sites, especially for users using VOIP or video conferencing technologies.

2. Purpose Statement

The purpose or this research is to implement and evaluate IEEE 802.21 in HFNs in order to allow more mobility to users inside the conversation space, as well as to reduce the time and trouble needed to move between heterogeneous networks.

C. LITERATURE REVIEW

Silva, Carvalho, Sousa, and Neves (2011) list the reasons behind the creation of the MIH. The first is the growing number of mobile devices that support multiple radio technologies, such as Wi-Fi, WiMAX and 3G. The second reason cited by Silva et al. is the increasing tendency toward adopting new computing paradigms such as cloud computing, which makes the user wants to be "always best connected." The third reason is the extensive deployment of wireless networks in many places, such as enterprises, public places, and homes, which, most of the time, overlap. Usually in that case, the user prefers to be connected to a faster and cheaper network (Lim, Kim, Suh, & Won, 2009). The final reason is the tendency of converging communications networks, as shown by most services providers and manufacturers.

In these circumstances, IEEE 802 has created Working Group (WG) 21 (802.21) in order to elaborate a protocol that allows the user to seamlessly roam across heterogonous networks. It was called the "Media-Independent Handover." Taniuchi et al. (2009) tried to show the importance of standardization for a handover protocol. He compared the scalability of a media-independent framework and the solution that suggests the creation of "media-specific extensions" for each technology. The comparison favored the first solution. because its complexity increases by an order of N, whereas the complexity of the second approach grows by the factor of N^2. Another important factor is that MIH is "unique" compared to other IEEE protocol, because it provides handover between IEEE 802 technologies (802.11, 802.3 and 802.16) and cellular networks such as 3GPP and 3GPP2.

Many efforts were made to evaluate, improve, and test some MIH implementations. Piri and Pentikousis (2009) did one of the first tentative implementations of IEEE 802.21. The proposed prototype covers all components and services described by the MIH standard that facilitate seamless handover across heterogeneous technologies. Moreover, Piri and Pentikousis (2009) suggested the use of their solution to adapt network applications according to the status of the link and network. The example proposed was the use of the Skype application program interface

(API) to control Skype behavior during a voice-over-IP (VOIP) session, according to information obtained from the Media Independent Information Service (MIIS) server.

Lopez, and Robert (2010) proposed another open-source implementation for IEEE 802.21, called OpenMIH. This implementations aims to prepare secure handover across different network technologies. The software was tested in an illustrative scenario for "proactive pre-authentication" in a wireless-based network (Lopez, Y., & Robert, 2010).

Silva et al. (2011) tried to implement and test a mobility solution based on IEEE 802.21 and Fast Mobile IPv6 (MIPv6) in Android-based devices. The test bed was designed to evaluate handovers from 3G networks to Wi-Fi networks, and vice versa. Modifications were made to the basic Android OS in order to support IEEE 802.21, MIPv6, and to communicate with the external network mobility manager (NMM) that initiates the handover (Silva et al., 2011).

Another implementation that aims to integrate IEEE 802.11/802.16e using IEEE 802.21 was designed and implemented by Lim et al. (2009). They deployed an IEEE 802.21 to evaluate its performance by measuring (i) packet loss, (ii) handover latency, and (iii) access-point (AP) discovery time and power consumption. The tests supported all service types introduced by MIH, which are MIES, MICS and MIIS. It has even introduced a new entity called "connection manager" (CM), responsible for AP discoveries and support of seamless vertical handovers. According to Lim et al. (2009) the results of the tests showed reduction in the packet loss during handover, reduction of handover latency, enhanced AP discovery, and efficient energy consumption.

Cicconetti, Galeassi, and Mambrini (2011) proposed another software implementation of IEEE 802.21. It has also implemented an MIIS server in order to evaluate network-assisted handovers. The experiment has two main objectives. The first is the realization of smooth horizontal and vertical handover. The second is reducing the energy consumption of the mobile nodes due to scanning. The results were "promising," because the prototype tested showed not only an increase in handover latency but also efficient energy consumption, by removing scanning for networks in the mobile node due to use of MIIS server.

Mussabbir and Yao (2006) proposed an architecture based on IEEE 802.21 and Fast Mobile IPv6 (FMIPv6). The tests realized had as main objective to enhance and optimize the handover mechanism with the support of IEEE 802.21 services. Mussabbir and Yao (2006) implemented a software solution for the MIIS service defined in the MIH standard and added a new information report they called "heterogeneous network information" (HNI). The new information report contains Layer 2 (L2) and Layer 3 (L3) data concerning all neighboring networks.

Corujo et al. (2011) presented an open-source implementation of 802.21 called ODTONE (Open Dot Twenty ONE). The architecture described in the paper involved integration between ODTONE and an open-source implementation of Proxy Mobile IPv6 (PMIPv6), called OPMIP, in order to create "make-before-break" network-initiated handovers. The results showed the ability of ODTONE to enhance and complement PMIPv6, achieving "an optimized, network-based, localized mobility management" (Corujo et al., 2011).

D. RESEARCH QUESTIONS AND HYPOTHESES

In this research we will try to answer the following questions:

1. How can we implement MIH in HFN?
2. What are the benefits of the integration of MIH in HFNs?
3. Will the implementation of MIH improve the quality of service in HFN?
4. Will the implementation of MIH improve the quality of user experience in HFNs?
5. Will the implementation of MIH improve the mobility and the connectivity inside the conversation space?

E. THESIS ORGANIZATION

Chapter I: Introduction. This chapter gives a general outline of the problem with a description of the research motivation and questions that will be answered.

Chapter II: This chapter discusses the current state of hastily formed networks. It will describe the main technological features and challenges of HFNs.

Chapter III, describes MIH 802.21—its features, functionalities, and challenges. It also includes a detailed description of ODTONE architecture.

Chapter IV describes in detail the experiments done in the field and laboratory using ODTONE and SIP.

Chapter V concludes by summarizing key findings and conclusions drawn from this thesis and expressing recommendations. Future research in this topic area is also proposed.

THIS PAGE INTENTIONALLY LEFT BLANK

II. HASTILY FORMED NETWORKS

A. BACKGROUND AND DEFINITIONS

1. Background

The hastily formed network (HFN) system was developed and has been deployed by the Naval Postgraduate School (NPS) for several years, and has included students and faculty from several departments, as well as many industry experts, among its researchers. The first major NPS deployment in support of a humanitarian assistance/disaster relief (HA/DR) effort was in Bay St Louis and Waveland Mississippi, to assist in HA/DR efforts after Hurricane Katrina devastated much of those two cities and the surrounding communities.

2. Definition

After a disaster, first responders need to communicate among each other in order to improve their situational awareness and share information. HFN was created for this reason, connecting all responders and providing them with a platform that enables information sharing, reliable communication (video/audio), and an improved decision-making processes.

Denning (2006) states that an HFN consists of five components:

(1) A network of people, established rapidly, (2) from diverse communities, (3) working together in the same conversation space (4) in a way in which they plan, commit to, and execute actions, to (5) fulfill a large, urgent mission.

However, Denning claims that these elements are not enough, because in his opinion, many organizations using advanced technologies in a disaster area don't necessarily lead to successful operations. An HFN is therefore more than a group of organizations deploying advanced networking technology in order to communicate and coordinate.

Nelson, Steckler, and Stamberger (2011) provide another definition of the hastily formed network:

Hastily formed networks (HFNs) are portable IP-based networks that are deployed in the immediate aftermath of a disaster, when normal communications infrastructure has been degraded or destroyed. Since HFNs create new communications infrastructure, they can be very valuable in providing basic communications (voice/video/data) until pre-disaster infrastructure can be restored. HFNs are a particularly effective implementation of information and communication technology (ICT), enabling the crisis communications necessary for a rapid, efficient, humanitarian response.

3. Conversation Space

Denning (2006) defines the conversation space as the medium where all the interaction between the early responders happens. The conversation space is formed by three principal elements, described in Figure 1.

Category	Characteristics	Examples
Physical systems	Media and mechanisms by which people communicate, share information, and allocate resources	Telephone, power, roads, meeting places, supplies, distribution systems
Players	Players included and their roles, core competencies, and authorities	Citizens, fire department, policy department, highways department, federal emergency management agency
Interaction practices	Rules of the "game" followed by the players to organize their cooperation and achieve their outcomes	Situational awareness, sharing information, planning, reaching decisions, coordination, unified command and control, authority, public relations. (Note: environment has no common authorities, no hierarchy, many autonomous agents, decentralized communications)

Figure 1. Components of the Conversation Space (Denning, 2006)

B. HFN ARCHITECTURE

Steckler (2012) describes all HFN components and their interaction in the HFN puzzle (see Figure 2), which describes all the resources, technologies, and assets needed during HA/DR operations.

Nelson et al. (2011) provide a layered architecture of HFN, as displayed in Figure 3. The present research focuses on the network layer and the technologies and material used in this layer.

1. The Physical layer

The physical layer deals with basic requirements to build an HFN, such as power sources and physical security.

a. Power Sources

In order to deploy any technology solution, power sources are vital; but after most disasters, the infrastructure is completely destroyed. Thus, HFNs need to install and deploy their own power supplies. Nelson et al. (2011) suggest the use of solar, wind, crank, and fuel-cell solutions, because they are lightweight, easy to use and don't depend on fossil fuel, which can be rare or hard to reach in a disaster.

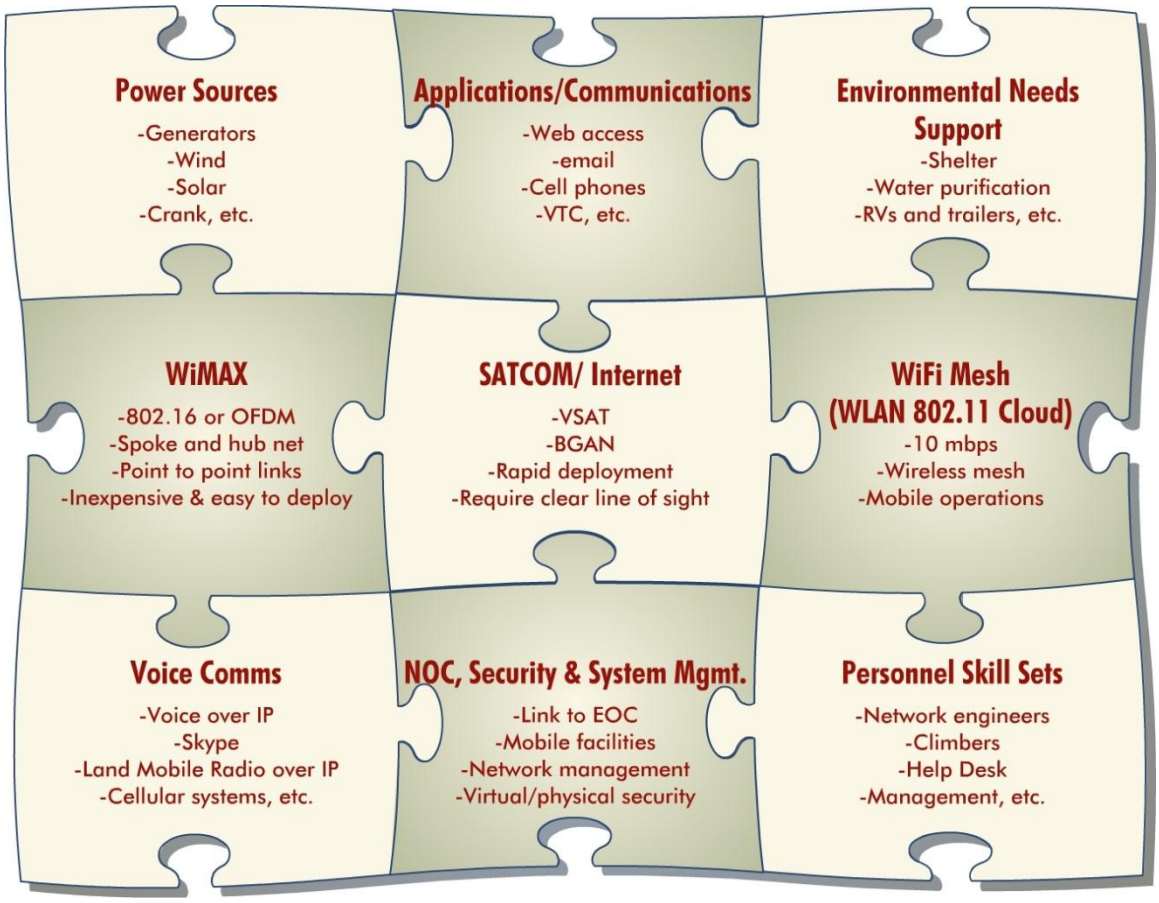

Figure 2. The Nine-Element HFN Puzzle (From Steckler, 2012)

b. Human-Support Needs

Early responders must be aware that basic human needs such as food and shelter will be scarce, as the chain of supply and local infrastructure will be destroyed in the disaster. It is important to decide how to get these supplies while deploying the HFN.

c. Physical Security

Physical security is very important, as it includes personnel security and the security of the local resources and material used to deploy the HFN. Nelson et al. (2011) emphasize this by reciting security problems that occurred in Haiti.

d. Network-Operation Center

Nelson et al. (2011) describe the network-operation center (NOC) as the central part, or brain, of the HFN. The NOC can be placed in a local building, tent, or mobile command. Its main mission is managing the RF spectrum and bandwidth and managing and securing wireless and SATCOM communications.

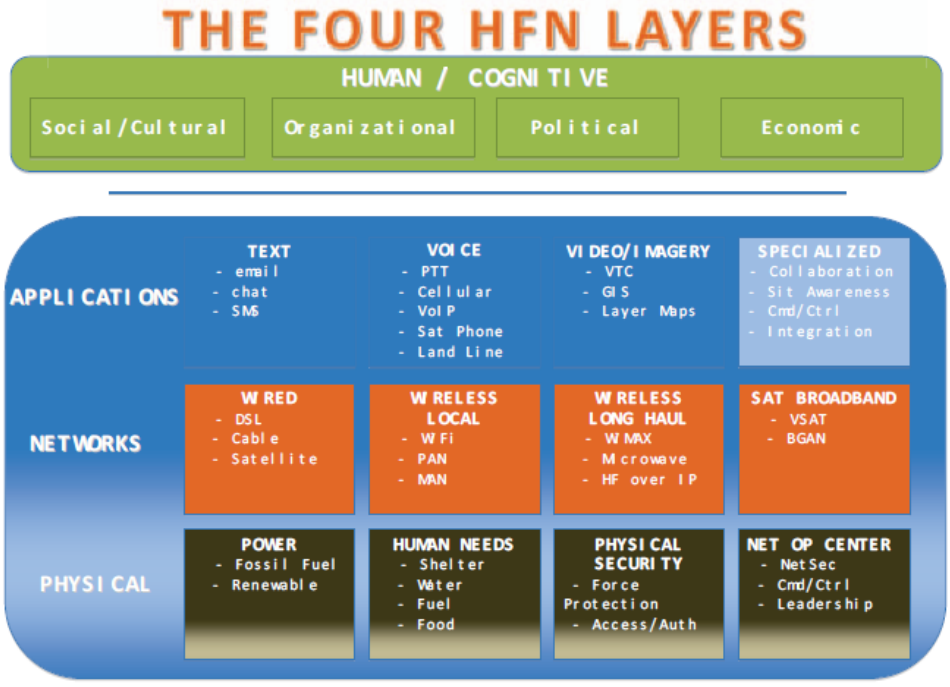

Figure 3. The Four HFN Layers (From Nelson et al., 2011)

2. Network Layer

The network layer is the most important, because it plays the role of backbone for all communications. There are no restrictions—any networking technology can be used—but this research will be interested in three technologies that are used in most HFN deployments: WiMAX, Meshed WiFi, and satellite communications.

a. WiMAX

The standard IEEE 802.16, or WiMAX, is short for "Worldwide Interoperability for Microwave Access" (an alternative name given by the industry group, WiMAX Forum). It is an attractive emerging metropolitan technology for rural and metropolitan-area broadband wireless access (BWA) that enables communication over long distances at high speed for residents and enterprises and supports a large range of applications for different environments. WiMAX provides an appropriate solution for some rural or inaccessible areas that are deprived of access to broadband Internet for cost reasons and provides a complementary solution to DSL (digital subscriber line) and cable networks. WiMAX enables interconnecting Meshed WiFi hotspots as well.

b. Satellite-Based Internet Access

Satellite communications (SATCOM) enable Internet connections when normal terrestrial infrastructure is down. SATCOM provides an easy and quick solution, as it can be deployed in less than an hour. Although it is expansive compared with other typical methods of Internet access, the satellite service offers a unique and effective solution in a disaster environment. VSATs (very small-aperture terminals), which range from 1–3 meters, and BGANs (broadband global-area network) satellite communications devices are another option, which are the size of a small case, are the commonly used portable satellite technologies. The VSAT and BGAN systems are packaged in one or two light transit cases, offering easy portability and deployment anywhere. The VSAT systems provide Internet access (up to 30 Mbps) operating on frequency bands X, C, Ku, and Ka. BGAN operates in L band. Satellite connections are not without issues in deployment and do present some problems, including (Nelson et al., 2011):

- "Rain fade," where the existence of a storm can degrade satellite service by affecting either the end-user ground terminal or the provider's earth station.
- Saturation of service capacity due to the use of too many terminals in one area, usually leading to service degradation
- Long-distance signal travelling in geosynchronous satellite communications causes latency and jitter, which affects network performance for certain time-demanding applications.

c. Wireless Area Networks (WLAN)/Meshed WiFi

IEEE 802.11 is used to provide Internet connection to different mobile devices in the conversation space. The interconnections of many wireless access points (WAP) will provides a meshed WiFi "cloud" that allows seamless mobility to early responders. The off-the-shelf equipment used supports different speeds (10–100 Mbps) and WiFi versions 802.11n/b/g.

3. The Application Layer

The application layer consists of all application and services running over the network (Wi-Fi/meshed WiFi). In the beginning of HFNs, the applications were basically text-based messaging, chatting, and basic web browsing (Nelson et al., 2011). As networking technology matured and throughput increased, early responders were able to profit from VoIP applications and services such as Skype.

The problem of interoperability among the radio technologies used (especially push-to-talk) by early responders led to the adoption of radio-over-IP (RoIP) systems (Nelson et al., 2011).

4. The Human Cognitive Layer

The Human cognitive layer is composed of four elements: organizational, economic, political, and social/cultural (Nelson et al., 2011).

- Organizational: Generally the absence of centralized command during HA/DR operations causes many interoperability problems. The key success of the operations is information sharing among all participants.
- Economic: The price of SATCOM connections and networking equipment can be unaffordable for some HA/DR organizations, which can negatively affect operations.

- Political: Government rules and policies that regulate the use of the RF spectrum can be challenging for early responders, because some frequencies and technologies are banned in some countries.
- Social/cultural: During huge disasters such as Katrina, the Haiti earthquake, and the Japanese earthquake, many organizations from different countries and various backgrounds get together. They usually have trouble communicating because of language barriers and cultural differences.

THIS PAGE INTENTIONALLY LEFT BLANK

III. IEEE 802.21 AND ODTONE IMPLEMENTATION

A. INTRODUCTION

Achieving seamless handover between heterogeneous networks requires taking into account certain considerations such as continuity of service, the type of application running on the network, quality of service (QoS), the discovery and selection of networks, security, and management of the energy consumption of the mobile system (Mohamad 2008). The IEEE 802.21 working group has created an architecture that defines a basic media-independent handover function (MIHF) that will help mobile systems do seamless handover between heterogeneous networks such as IEEE 802.3 (wired LAN), IEEE 802.11x (wireless LAN), IEEE 802.16e (mobile WiMAX network), GPRS and UMTS (3G mobile).

B. MIH OBJECTIVES

Initially, the IEEE 802.21 group set three main objectives (Corujo et al., 2011):

- Design a framework that enables transparent handover between heterogeneous technologies. This protocol should define new entities and the commands needed to optimize handover decisions.
- Define a new link-layer service access point (SAP) that is technology agnostic
- Implement new primitives and commands that will help mobility management protocols (such as MIP, MIPv6, etc.) execute optimized handover decisions.

Additionally, other secondary goals where set, such as (Corujo et al., 2011):

- Session conservation: 802.21 aims to conserver the session during and after the handover.
- Providing information and commands that make applications "handover-aware."
- Creating quality-of-service -aware applications
- Improving network research and discovery by providing information about available networks and characteristics

- Improving network selection. Network selection depends on factors such as QoS, cost, and link status. Thus, it can be improved if the MN get those information from an Information Server (IS)

1. Improving power management when the device is provided by a network map describing network cost, throughput, and link quality.

C. PRESENTATION OF THE IEEE 802.21 STANDARD

1. General Architecture

This section presents the general architecture of the IEEE 802.21 standard (also referred to as the media-independent handoff (MIH)), providing a description of all the different entities introduced by this protocol, as well as their interactions.

Figure 4 is an overview of the general architecture of the MIH framework as defined by IEEE 802.21 standard (Lopez & Robert, 2010). The figure shows a MN that has two interfaces, a 3GPP interface and an 802 interface that is connected to the network. It shows also the intern architecture of the 802 network (which can be an access point) and the 3GPP network (the base station). All the nodes displayed in the figure have a central entity MIHF. The MIHF provides services to the upper layers through interfaces that are technology independent. It obtains information from the lower layers through many interfaces or technology-dependent SAPs. This information is used by the MIH users to make better handover decisions. The communication between MIHF and the MIH users and between MIHF and lower layers is done through the use of SAPs. The current version of IEEE 802.21 defines three types of SAPs.

- MIH_SAP: used for communication between MIH users and the MIHF
- MIH_LINK_SAP: used for communication between the MIHF and lower layers
- MIH_NET_SAP: used for the exchange of information between remote MIHFs

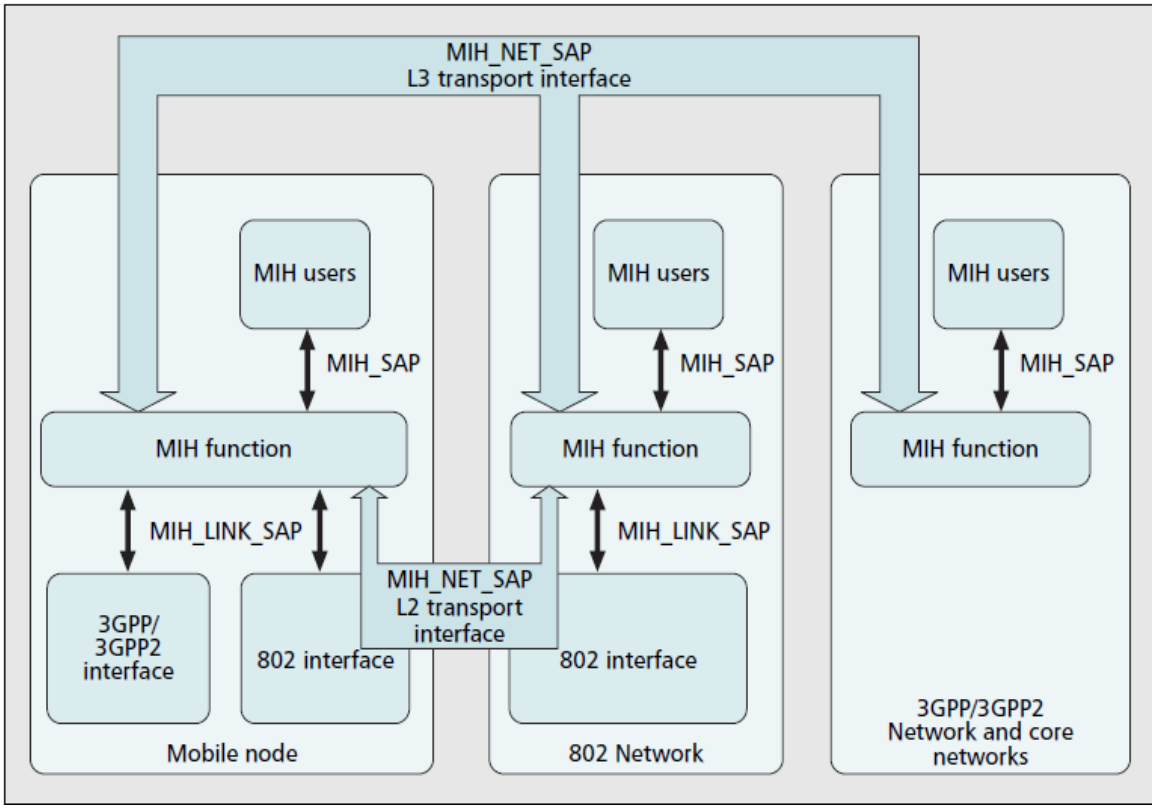

Figure 4. General Architecture and Interaction Between Entities (From Corujo et al., 2011)

In the context of MIHs, there are two types of entities. Non-MIH entities are managed by a third party. MIH entities implement the standard. All these entities and their interactions are represented in Figure 4, which is a reference model for 802.21 (Corujo et al., 2011).

- MIH point of service (MIH PoS): "a network entity that exchanges necessary MIH messages with MNs" (Corujo et al., 2011). A PoS can communicate with many MNs at a time and, as shown in Figure 5, a MN can communicate with many PoSs.
- MIH point of attachment (PoA): can be an access point (AP) or a base station (BS).

Figure 5 also shows the communications between the previously described nodes. These communications are called communication reference points (Corujo et al., 2011):

- R1 (MN <-> Serving PoA): describes the communication and messages between the MN and its point of attachment. Its main goal (in the context of MIH) is to get information about the connection state.

- R2 (MN <-> Candidate PoA): describes the communication of MN with other or candidate PoAs. Its main goal is to obtain information needed for handover decisions.
- R3 (MN <-> non-PoA): describes the interaction between the MN and another network entity (it can be also an entity from a foreign network). It provides the MN with information about the other network.
- R4 (PoS <-> non-PoS): This communication reference point describes the communication between an MIH PoS serving a MN and another MIH non-PoS. The best example for this communication is between two information servers (one of them is the PoS for the mobile node)
- R5 (PoS <-> PoS): The last communication-reference point refers to the communication that happens between two PoSs from different networks.

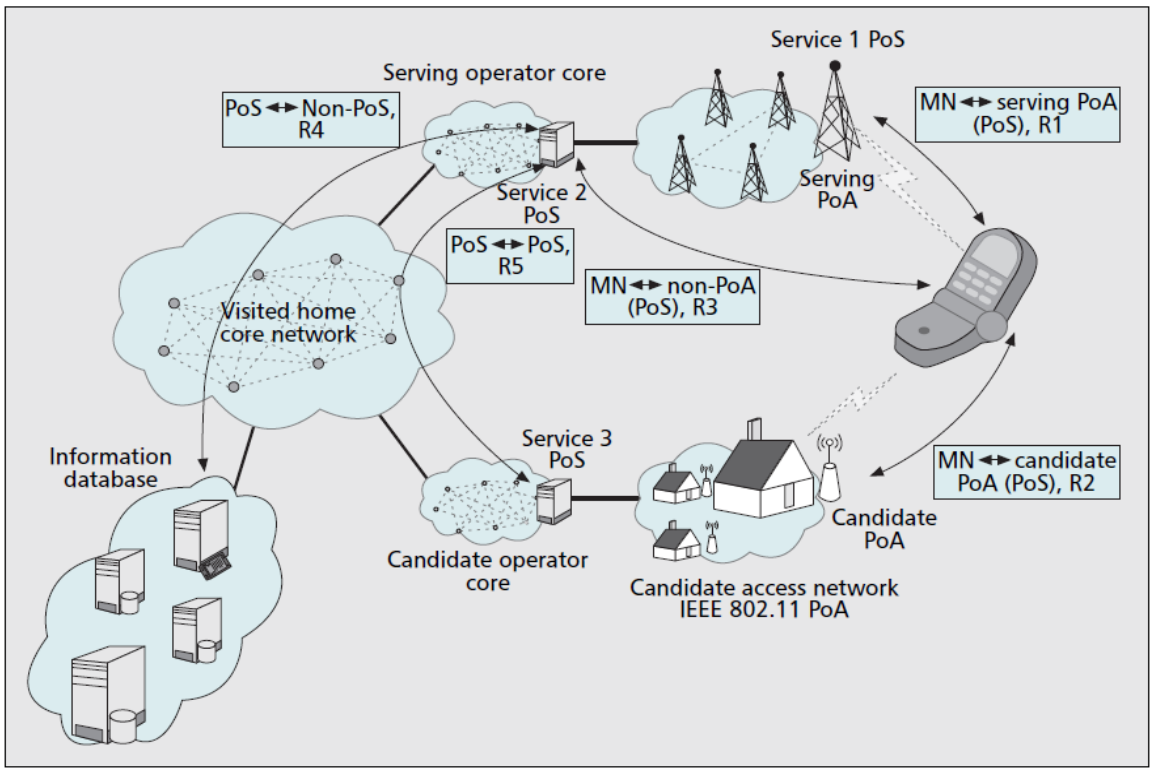

Figure 5. Reference Model (From Corujo et al., 2011)

D. MIH SCOPE AND INTEGRATION IN THE PROTOCOL STACK

There is a common misunderstanding that must be pointed out. IEEE 802.21 does not execute handovers and do not define handover policies. It does not control network detection and does not specify network-selection procedures. However, it specifies

procedures that facilitate handover decisions by providing information about the link state to MIH users, which helps minimize the handover latency. It defines the methods and semantics that facilitate obtaining network information, and thus optimizes the detection of the available networks.

Figure 6 shows the scope of MIH as defined by the IEEE 802.21 standard. One of the biggest concerns about IEEE 802.21 is how to integrate it into our current systems and what modifications are needed to support this standard.

Eastwood et al. (2008) illustrate how to fit IEEE 802.21 in the protocol stack of a multimode client in Figure 7. The standard can be seen as another layer, which some people label as Layer 2.5 because it is between the link layer and the network layer. The integration and support of MIH has already started, because the 802.11 and 802.16 (specifically 802.16g) working groups (WG) have changed the media-access control (MAC) layer specifications in order to support MIH (Eastwood, L et al., 2008). For instance, the IEEE 802.11u WG has integrated new functions in its MAC state machine in order to support and provide services to 802.21.

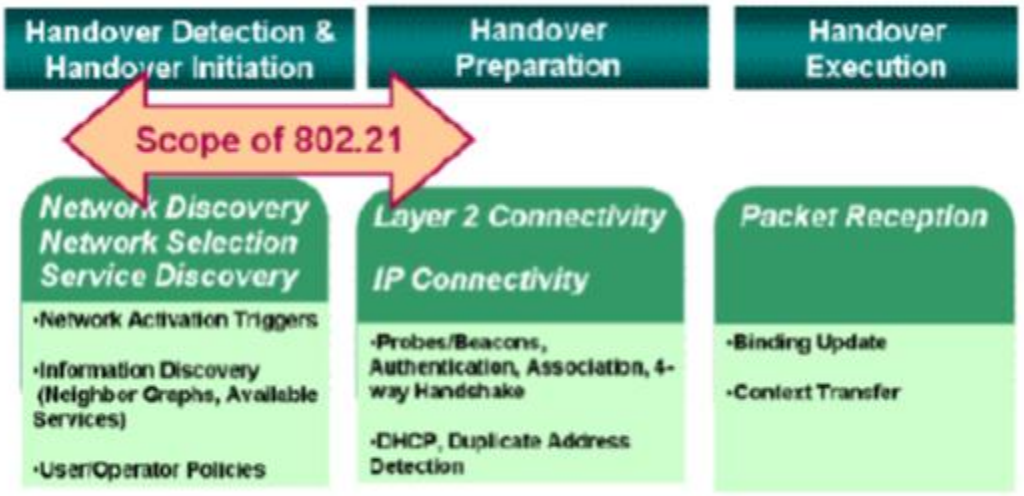

Figure 6. MIH scope (From Mohamad, 2008)

The IETF also started the change toward the support of IEEE802.21. In fact, the IETF MIP-SHOP (Mobility for IP: Performance, Signaling, and Handoff Optimization) is

now changing Layer 3 in order to support MIH and carry the IEEE 802.21 payloads for faster and better handover (Eastwood, L et al., 2008).

E. MIH SERVICES

The IEEE 802.21 standard requires that MIH users register to an MIHF in order to benefit from its services. Three services are defined by the standard: media-independent event service (MIES), media-independent command service (MIHCS), and media-independent information service (MIIS). These services will be presented in the next sections.

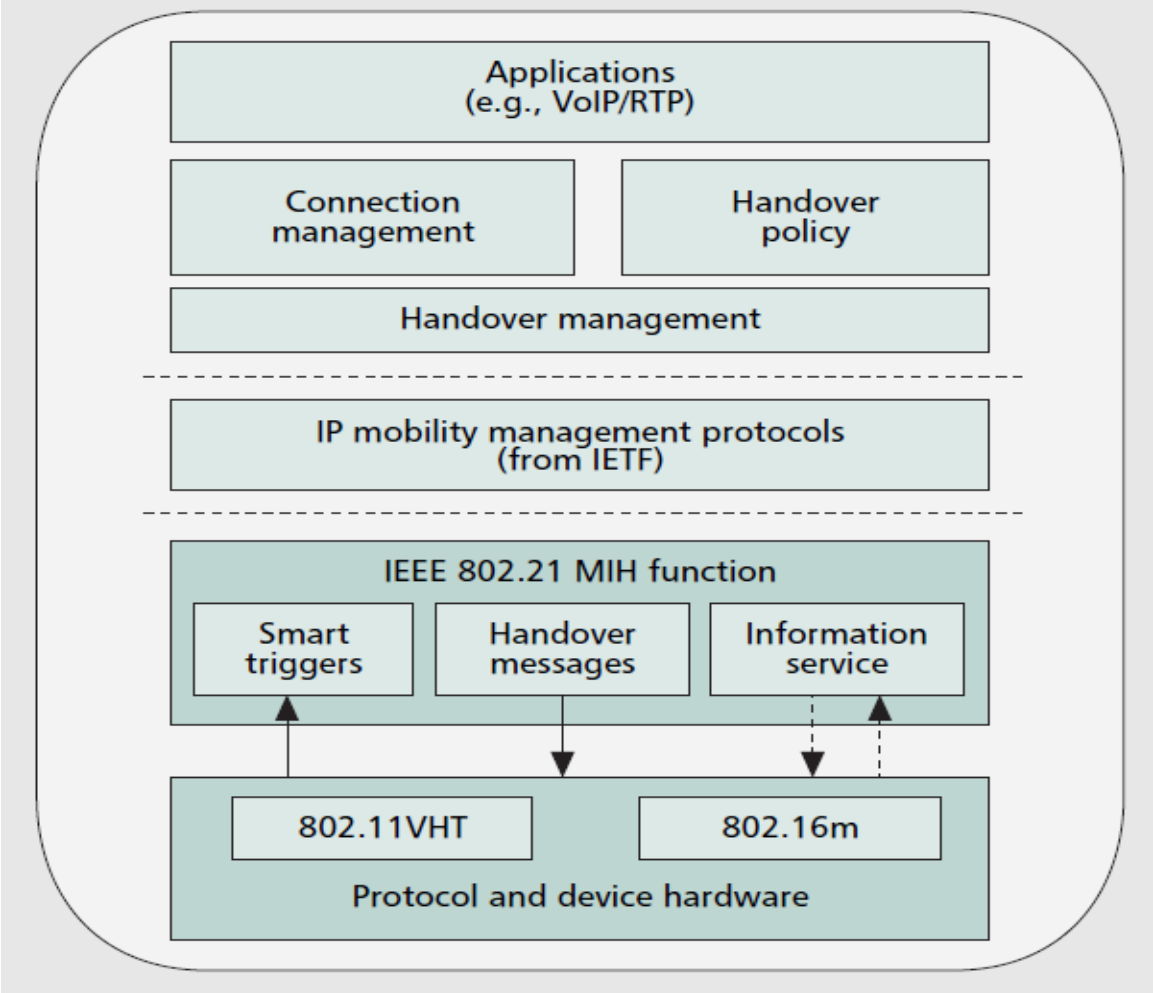

Figure 7. Example of IEEE 802.21 Implementation (From Corujo et al., 2011)

1. MIH Independent-Event Service (MIES)

In general, the handover can be initiated by either the mobile node or the network (Mohamad, 2008). The events that can initiate a handover may come from the MAC layer, PHY, or MIH function. This depends on the mobility of the MN, or state changes in the environment (network bandwidth changes, link-state changes, etc.) or the policy of management of the network. Those events or changes can be local or distant. Remote events can be delivered using the reference points R1, R2, and R3, explained previously. According to Corujo et al. (2011), the events are divided into two types: link events and MIH events. Link events are exchanged between the lower layers (link layer and below) and MIHF, whereas MIH events are exchanged between MIHF and MIH users. The flow of events (MIH and event) is shown in Figure 7.

2. Media-Independent Command Service (MICS)

The command service manages commands from the upper layers to lower layers of the reference model (Piri and Pentikousis, 2009). The upper layers and other users can use MICS commands to determine the states of the links and/or control optimize performance of the multi-modal terminal. Service commands can also allow users to execute a seamless and optimal handover, since the commands include useful information such as signal strength, throughput, etc. As for events, there are two types of commands: MIH and link (Corujo et al., 2011).

- MIH commands: these commands are sent by MIH users (Figure 6) to the MIHF. These commands could be sent locally or destined to remote entities.
- Link commands: these are sent from the MIHF to lower layers. Link commands can only be local and are specific to the Layer 2 technology used.

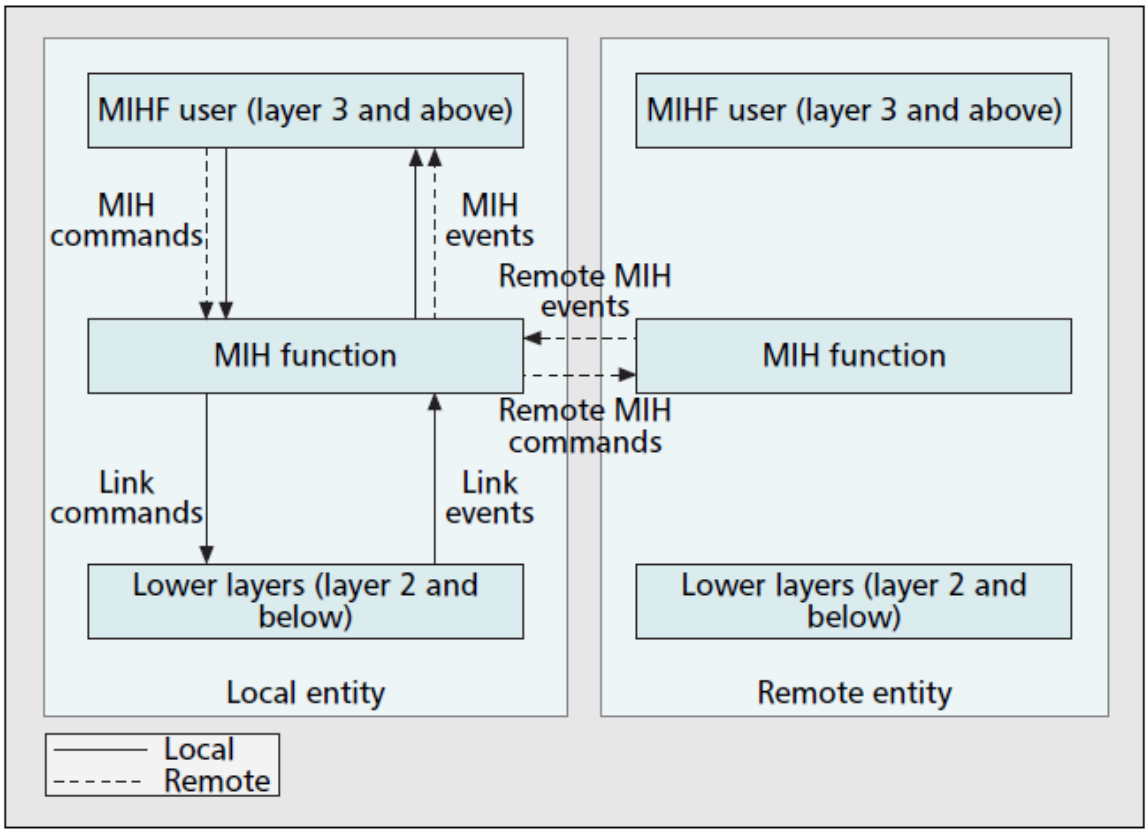

Figure 8. Event, Command And Information-Services Flow Mode (From Corujo et al., 2011)

3. Media-Independent Information Service (MIIS)

The MIIS provides the MIHF with nearby network information in order to make handovers easier. It provides a network map of the area of interest of the MN. The network map consists of set information elements (IEs) (Lopez and Robert, 2010). IEs can provide information from lower layers such as link parameters, coverage, and neighboring networks map (Corujo et al., 2011) as well as higher layers, such as network cost, services available, and Internet availability.

Information Element	Category	Description
IE_OPERATOR_ID	General IEs	Identifier of operator, can be a domain name
IE_COST	Access Network Specific IEs	Monetary cost
IE_NETWORK_QOS		Link Layer QoS of access network
IE_NETWORK_DATA_RATE		Max value of access n/w data rate
IE_NET_FREQUENCY_BANDS		In KHz for broadband and cellular networks
IE_NET_IP_CFG_METHODS		DHCP, Foreign Agent, etc. along with their IP addresses, Helpful in IP acquisition
IE_NET_CAPABILITIES		Internet access, MIH Capability, etc.
IE_NET_MOB_MGMT_PROT		Proxy-based mobility protocols
IE_POA_LINK_ADDR	Point of Attachment (PoA) Specific IEs	IEEE MAC address
IE_POA_CHANNEL_RANGE		Channel range in which PoA is communicating

Figure 9. Information Elements (From Mohamad, 2008)

F. IEEE 802.21 SCENARIOS

According to (Mohamad, 2008) MIH divides the handover operation into three phases: first, the initiation; second the preparation; and finally, the execution. As mentioned before, MIH doesn't execute handover; this phase is executed by other mobility-management protocols, such MIP, MIPv6, and SIP. The handover initiation phase starts when some link-layer parameter such as links going down, packet-error rate or lost rate is increasing (Mohamad, 2008). Then the handover preparation phase starts by gathering information about available networks in the area and their characteristics.

The information exchanged during these phases and the entities involved depend upon the MN and the access technology used. Different handover scenarios are defined by IEEE 802.21 (Ohleger Jr., 2012).

1. Scenario Classes

Different handover scenarios defined by the IEEE 802.21 standard are classified into 4 main classes (Ohleger Jr., 2012):

- Class 1: The MN and the network implant MIH. In this case, the handover will follow the procedure recommended by the standard.
- Class 2: The MN implants MIH, but not the network controller. Handover (if possible) will be initiated by the MN.
- Class 3: The network controller implements MIH, but not the MN. The handover (if possible) will be initiated by the network controller.
- Class 4: Neither the mobile or the network implanted MIH: in this is impossible.

2. Scenarios for the implementation of MIH

The IEEE 802.21 standard proposes five possible implementation scenarios (Ohleger Jr., 2012):

- Scenario 1: IEEE 802.11x <=> IEEE 802.16e. A multi-mode station is connected to the intranet IEEE 802.11x. It crosses the campus to another building. Between the two buildings, intranet connection is in IEEE 802.16.
- Scenario # 2: IEEE 802.x <=> 3G. A multi-mode station is connected to the intranet IEEE 802.x. The user wants to continue a session on a GPRS / UMTS network or vice versa.
- Scenario 3: IEEE 802.11x <=> IEEE 802.11y A MN is connected to the Internet from a public hotspot IEEE 802.11 in a hotel. The user starts a videoconference then moves to another 802.11 hotspot, but with a different extended service set (ESS). He wants to continue the session without interruption.
- Scenario # 4: IEEE 802.11x <=> 802.11y IEEE or IEEE 802.11z. An MN is in an airport and sees several service-set identifiers (SSIDs) possible to create an association network—which one is best to choose?
- Scenario # 5: IEEE 802.3 <=> IEEE 802.11x A multi-mode station is connected to a LAN and wants to switch to the available 802.11x hotspot while conserving the session.

3. Use Case: Inter-Technology Handover Using MIH and MIP

Figure 10 illustrates an example of a seamless handover procedure from 3G to WLAN. The mobile node is supposed to have MIH and MIP implemented and supported:

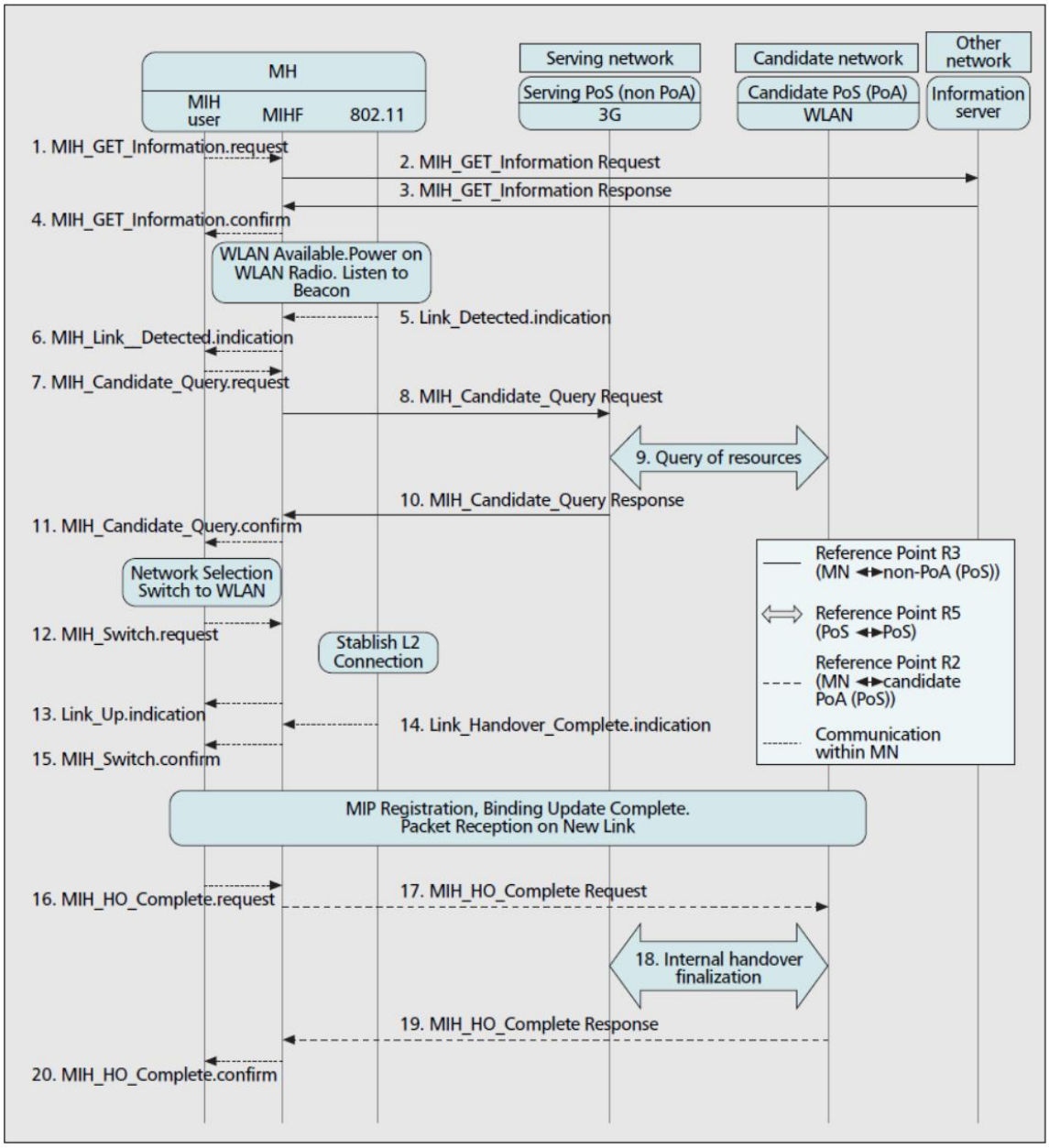

Figure 10. Inter-Technology Handover (From Corujo et al., 2011)

- The MN wants to know about the networks available in its area, so it queries its MIHF (message 1), who sends a query to the MIIS server located in a third party (can be the service provider). The MN gets the

necessary information in Message 4, then it switches its WLAN interfaces because there is a WLAN available in the area.

- When the 802.11 interface detects the wireless network available (by listening to beacons) it generates Message 5 (MIH_LINK_SAP), informing the MIHF about the available network, which generates Message 6 (MIH_SAP) to inform the MIH user about this network.
- The MN triggers the handover procedure when it receives Link_detected.indication (Message 6) by sending the information about the new available network to its PoS (in 3G network). This information reaches the PoS through messages 7 and 8.
- The PoS starts a communication (Messages 9) with the PoS of the candidate network after getting Message 8 from the MN. The serving 3G PoS tries to get more information about the WLAN and the other surrounding networks, then its sends it to the MN (messages 10 and 11).
- The information received helps the MN make a decision about which network is better (regarding many factors such as cost, QoS, throughput, etc.). After the decision is made, the MIH user sends a switch command to the MIHF (Message 12). This will trigger the connection to the selected 802.11 network. After establishing the network connection, the Layer 2 (802.11 interface) sends Message 14 (Link_handover_ complete.indication) to inform the MIHF that the L2 handover is done. The message is fthen orwarded to the MIH user (message 15).
- The reception of Message 15 triggers the handover in higher layers. In this scenario, Message 15 will trigger a Layer 3 handover using MIP. Any other mobility-management protocol can be used during this operation.
- When the MIP handover procedure is completed, the MIH user sends Message 16 (MIH_HO_Complete.request) to inform the MIHF, which forward the message to the new PoS (WLAN PoS). Then PoS inform all the concerned PoAs and PoSs that the handover is successful and that it is now the serving PoS for the MN.
- To close the handover procedure, the PoS sends Message 19 to the MIHF forwards it to the MIH user.

G. ODTONE

In this section we will describe and present an open-source framework implementation of IEEE 802.21.

1. Related works

De La Oliva, et al. (2008) state that there were many attempts to implement IEEE802.21. One of the first implementations attempted to optimize SIP-based handoff. While it implemented many MIH functions and capabilities, this implementation wasn't "publicly disclosed" (De La Oliva et al., 2008). Another implementation based on Gnu/Linux (Muhammad, 2009) was released in 2009. Yet it only focuses on Linux products and does not support 3GPP. De La Oliva et al. (2008) presents a better implementation that is written in C and runs as a configurable network daemon on the Linux operating system. Although it presents a better implementation by supporting a larger number of MIH functions, it still lack support for different operating systems. Corujo et al. (2011) claim that the best available open-source implementation is Open Dot Twenty (ODTONE), because it provides a framework that implements most MIH capabilities and services and runs on different operating systems such as GNU\Linux systems, windows-NT and Android devices.

In the next sections, ODTONE architectures and main features are presented.

2. Architecture

Carlos and Bruno (2012) define ODTONE as an open-source attempt to implement IEEE 802.21 using C++ API (especially the Boost library). ODTONE supports all MIH services and most of its mechanisms, such as capability discovery, MIHF registration, event registration, etc. ODTONE developers claim that one of the most important features of this implementation is its being technology independent and allowing developers to implement their own MIH_SAP and MIH_LINK_SAP (Corujo et al., 2011).

A detailed ODTONE architecture is shown in Figure 9 (Corujo et al., 2011). ODTONE is composed of the following software modules (Corujo et al., 2011):

- Communication handler: A point of contact between all software components and modules. It collects Information, which is exchanged in the form of messages, from different SAPs and other (remote) MIHFs and forwards them to the service-access controller.

- Service-access controller: Forwards MIH messages to the concerned MIH service (MICS, MIES, or MIIS) after analyzing the message header
- Link manager: responsible for the selection and acknowledgment of the MIH-users that will interact with the MIHF
- Transaction-state machine controller: responsible for observing the status of communication with remote MIHFs

Other than these functions, ODTONE implements the basic service describes by IEEE 802.21 standard in separate software components:

- MIES component: offers functions for management of event subscription, event validation, and event publication. The standard proposed an architecture similar to the publish-subscribe architecture, so MIH-users has to subscribe to desired events that are published by the MIHF. This module allows the MIHF to manage subscriptions and subscribed users.
- MICS component: similar to MIES, this module has its own command validation and publishing functions. The validation function is used to verify the conformity of the received commands the standard.
- MISS component: Although the definition of an IS server or service is out of the scope of the standard, the ODTONE development team provided a basic implementation of an IS server that supports some IEs.

We will provide a detailed description of the installation and configuration of ODTONE 0.4 in the final chapter.

3. Implemented Functions:

ODTONE is one of the best implementations available for IEE802.21, because it implements most MIH services and functions. ODTONE developers aimed to give developers a framework that help developing applications that support MIH. That is why ODTONE implements only the MIHF core functions, such as MICS and MIES, and gives to the developer the freedom to develop MIH users and LINK_SAP depending on the mobility-management protocol (using SIP, MIP, MIPv6, etc.) and the technology used (802.11, 802.16, etc.).

The current version of ODTONE provides MICS and MIES core functions and services. The MIIS is not fully developed; there is an implementation sample provided that supports some IEs. The MIH users provided with the latest version of ODTONE are just demonstration programs that display the message exchange between the network

entities. Also, there is only one 802.11 LINK_SAP that is fully developed and functioning. For this reason, our tests will focus on establishing seamless handovers between two 802.11 networks.

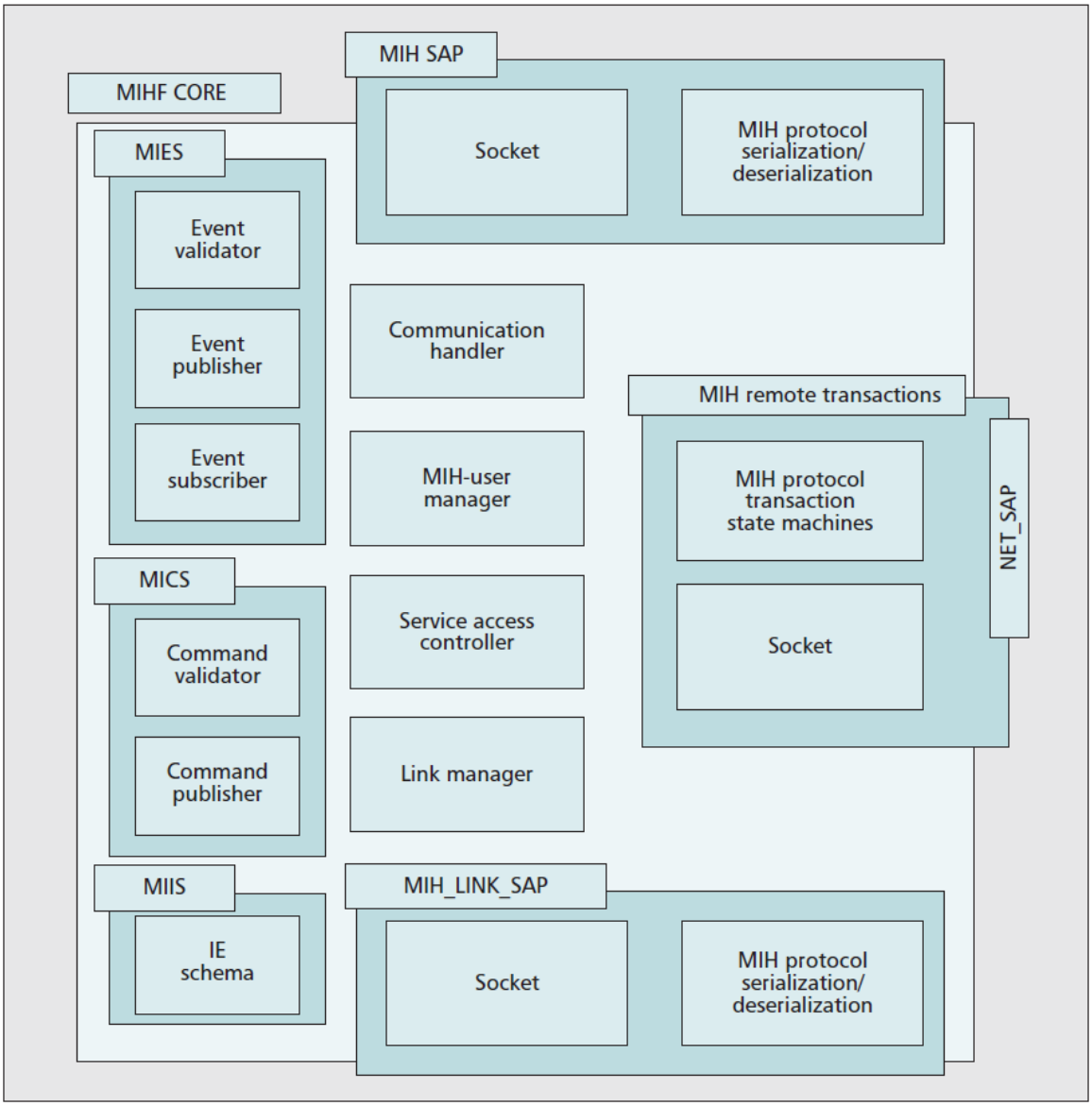

Figure 11. ODTOONE Architecture (From Corujo et al., 2011)

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EXPERIMENTION WITH SIP AND 802.21

A. INTRODUCTION

SIP stands for Session Initiation Protocol. It was created to set up, maintain and tear down multimedia conversations between two users in an IP-based network (SIP Tutorials, 2009). It allows a participant in a conversation to manage instant messaging or make audio and video calls. SIP was standardized by the IETF, first defined by RFC 2543 and then modified and updated many times subsequently (SIP Tutorials, 2009). The current version of SIP is defined by RFC 3261 (2002), which describes SIP as:

> …an application-layer control protocol that can establish, modify, and terminate multimedia sessions (conferences) such as Internet telephony calls. SIP can also invite participants to already existing sessions, such as multicast conferences. Media can be added to (and removed from) an existing session. (SIP: Session initiation protocol, 2002)

RFC 3261 defines four basic and principal functions that SIP must fulfill (SIP Tutorials, 2009):

- Locating users and resolving their SIP address to an IP address.
- Negotiating capabilities and features among all session participants.
- Changing session parameters during the call.
- Managing the set up and tear down for all users in the session.

B. SIP ENTITIES

The primary entities of the SIP protocol are called user agents. SIP protocol defines two types of user agents: user agent client (UAC) and user agent server (UAS) (SIP Tutorials, 2009). The UAC generates and sends requests to the server or to the UAS. The USA receives requests and commands, processes them, and then sends responses to the client or UAS.

1. Clients

The client is any network node that sends SIP requests and receives SIP responses (SIP: Session initiation protocol, 2002). The client is usually the user device that can initiate a conversation, and it can be a cellphone, PC or an IP-phone (SIP Tutorials, 2009).

2. Servers

RFC 3261 defines a server as a network node that receives a request, processes it, and then sends an answer to the client (SIP: Session initiation protocol, 2002). There are three types of servers.

a. Registrar Server

This server functions similarly to a DNS server because it stores names and addresses of the clients. Its database holds the location of the user agents within the domain and it responds to location requests (such as phone numbers or IPs) from other servers (especially proxy servers).

b. Proxy Server

This server handles call-routing authentication, loop detection per domain. It also accepts the initial user agent request to look up information (Module 8: Overview of SIP, 2012). After the communication starts, the proxy can stay in-path (not common) or drop out to allow UAs to communicate directly. The proxy can also play secondary functions, such as enforcing policies such as white and black lists (SIP: Session initiation protocol, 2002).

c. Redirect Server

The proxy server calls upon this server if the call is off-domain. If a user wants to call another user off-domain, he sends an "INVITE" message to the proxy, which then asks the redirect server about the end location. This server is used for mobile users whose locations keep changing.

C. THE SIP COMMAND AND MESSAGES

SIP is a text-based protocol that behaves like HTTP. SIP messages are exchanged between the client and the server. If a message is sent from the client to the server, it's called a request message. It is called a response message if it is sent from the server to the client (Module 8: Overview of SIP, 2012). The basic SIP message is constructed of "start-line, followed by one or more headers and a message body" (Module 8: Overview of SIP, 2012).

1. SIP Request Message

The following is an example INVITE request message sent by a SIP client to the server (SIP Tutorials, 2009):

```
INVITE sip:user2@server2.com SIP/2.0
Via: SIP/2.0/UDP pc33.server1.com;branch=z9hG4bK776asdhds Max-Forwards:
70
To: user2 <sip:user2@server2.com>
From: user1 <sip:user1@server1.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.server1.com
CSeq: 314159 INVITE
Contact: <sip:user1@pc33.server1.com>
Content-Type: application/sdp
Content-Length: 142
---- User1 Message Body Not Shown ----
```

The start-line consists of (Module 8: Overview of SIP, 2012):

- Method token: Identify the type of the request. The method token in this example is "INVITE." This indicates that the message captured is an invite request sent by a client to the server.
- Request URI: Identify the address of the receiver. In this example it is user2 on host server server2.com.
- SIP version: Identify the SIP version used.

RFC 3261 defines six methods (method token) that can be used in different types of requests. These methods are described in the RFC as following (Module 8: Overview of SIP, 2012).

- **Register:** This message is sent by UAC to inform the SIP server about its current location.

- **INVITE:** The conversation always starts by an INVITE message from the caller to the other end point.
- **ACK:** This is always sent as a response to an INVITE message.
- C**ancel:** Terminates a request. It is used if a client sends an INVITE and then changes its decision to call the recipient.
- **Bye:** This message is used to tear down a SIP session.
- **OPTIONS:** This message is used to obtain information about the capabilities of the server and/or any other device involved in the conversation.

Other RFC updates extend the request methods to thirteen methods by adding seven new ones (Module 8: Overview of SIP, 2012).

2. SIP Response Message

Here is the response to the aforementioned INVITE request (SIP Tutorials, 2009):

```
SIP/2.0                                200                                OK
Via:                                                              SIP/2.0/UDP
site4.server2.com;branch=z9hG4bKnashds8;received=192.0.2.3
Via:                                                              SIP/2.0/UDP
site3.server1.com;branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2
Via:                                                              SIP/2.0/UDP
pc33.server1.com;branch=z9hG4bK776asdhds;received=192.0.2.1
To:               user2              <sip:user2@server2.com>;tag=a6c85cf
From:             user1            <sip:user1@server1.com>;tag=1928301774
Call-ID:                               a84b4c76e66710@pc33.server1.com
CSeq:                            314159                            INVITE
Contact:                                              <sip:user2@192.0.2.4>
Content-Type:                                               application/sdp
Content-Length:                                                        131
---- User2 Message Body Not Shown ----
```

The start-line consists of (SIP Tutorials, 2009):

- SIP version.
- Status code: Three-digit number that indicates the outcome of the request. Equal to 200 in the previous example.
- Reason phrase: description of the outcome of the request such as OK, cancel, or bye.

SIP uses a response status code similar to the one used by HTTP protocol (SIP Tutorials, 2009):

- 1xx: Provisional -- request received, continuing to process the request;

- 2xx: Success -- the action was successfully received, understood, and accepted;
- 3xx: Redirection -- further action needs to be taken in order to complete the request;
- 4xx: Client Error -- the request contains bad syntax or cannot be fulfilled at this server;
- 5xx: Server Error -- the server failed to fulfill an apparently valid request;
- 6xx: Global Failure -- the request cannot be fulfilled at any server.

D. SIP MOBILITY

SIP can support different types of mobility such as terminal, session, personal, and service (Henning and Elin, 2000).

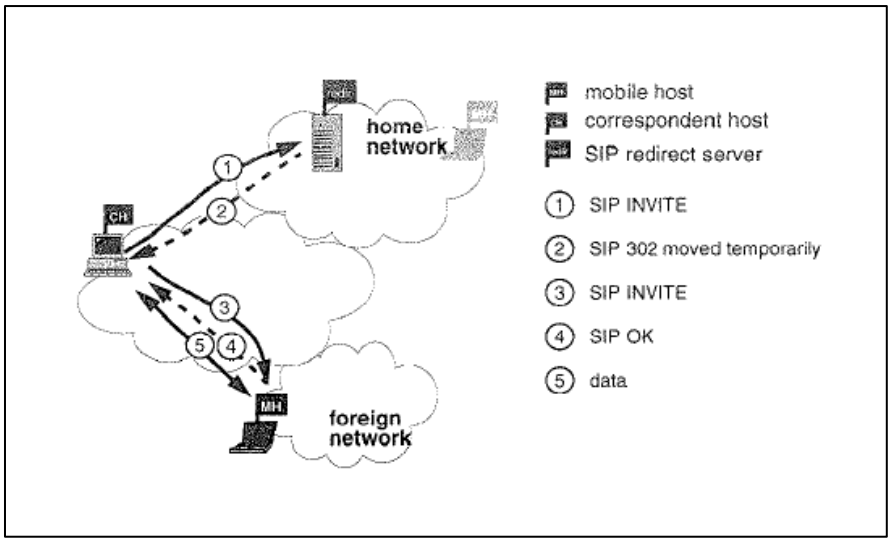

Figure 12. SIP-Based Pre-Call Mobility (From SIP: Session initiation protocol, 2002)

1. Personal Mobility

Personal mobility can be defined as the capability of being reached at different terminals using the same logical address or URI (Universal resource locator) (Henning S. & Elin W., 2000).

2. Session Mobility

Session mobility is defined by (Yeh, Wu, & Lin., 2006) as the ability to conserve the session while moving between different terminal devices.

3. Service Mobility

The authors of (Henning & Elin., 2000) define service mobility as the ability to providing access to the user even after he changes the terminal and service provider.

4. Terminal Mobility

Terminal mobility allows users to move between networks/subnets while maintaining the session (Henning & Elin, 2000). SIP can be used to support user terminal mobility in two different ways:

a. Pre-Call Mobility

This function is defined as the ability to move to another network/subnet, before making the call. This is considered the easiest type of mobility implemented by SIP (SIP: Session initiation protocol, 2002). The mobile host (MH) must register with the registrar server each time it moves from its "home network" to a "foreign network" (SIP: Session initiation protocol, 2002). Figure 12 illustrates this procedure of a corresponding host (CH) calling a MN that has moved to a foreign network.

b. Mid-Call Mobility

This function refers to the ability to maintain the session/conversation while moving between networks/subnets. The flow of this operation is illustrated in Figure 13, where MH and CH started the communication when MH was in Network A. The address of MH in Network A was 10.1.1.4. If MH decides to move to another network B, where it is assigned a new IP address 192.168.2.3, in order to maintain the conversation, it must inform the CH about its new location (new IP address). To this end, it sends a re-INVITE message (defined in Section 14 of RFC 3261 and updated/explained in RFC 6141) to the CH to inform it of the new IP address (192.168.2.3). When CH receives the message, it replies with an OK message to tell the MH that it knows about

the address change for the MN. Then, the MH sends an ACK message to acknowledge the received OK. Finally, the CH modifies the IP address of the MH in the SDP (Session-Description Protocol) in order to reestablish the multimedia session (Yeh,, Wu, & Lin, 2006).

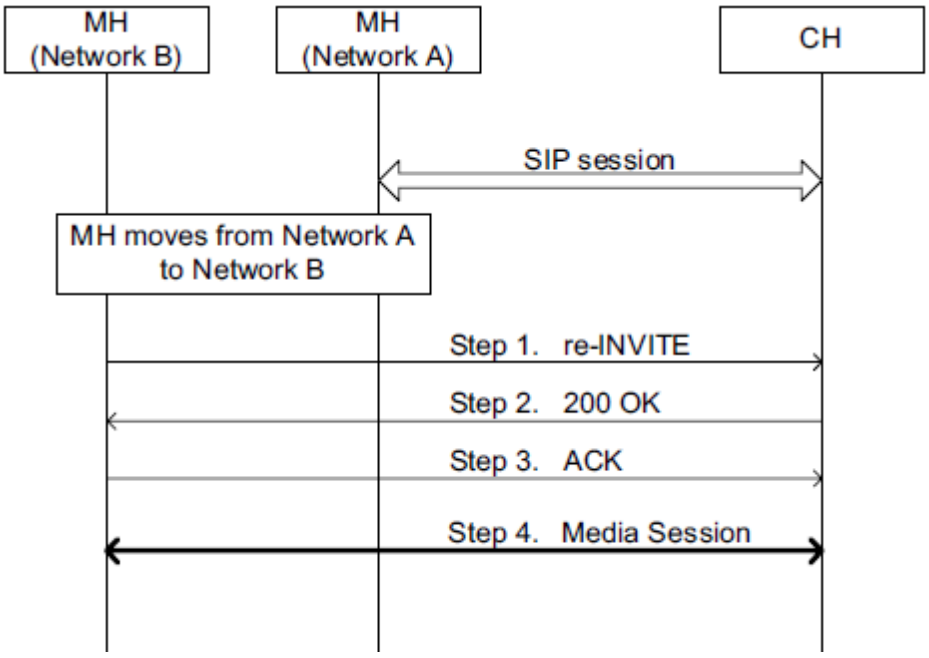

Figure 13. SIP-Based Mid-Call Terminal Mobility (From Yeh, Wu, & Lin, 2006)

E. EXPERIMENTATION WITH SIP MOBILITY AND ODTONE

1. Test-Bed Platform

In this experiment, we aim to implement and test the SIP-based, mid-call terminal mobility. The test consists of starting a multimedia session between two nodes (the MH and CH) and then moving the MH from his home network to another foreign network. The hardware platform and different software packages used for this test are as follows:

a. Software

- Operating Systems: Linux Ubuntu 3.2.0 for most tests and Windows 7 for one test with the Windows messenger software.

- SIP server: Kamailio 3.3.0, which is an open-source SIP server released under GPL (http://www.kamailio.org/w/).
- UA: linphone 3.3.2, Jitsi 1.0, Ekiga 3.3.2 or Windows messenger 5.0,
- Network sniffer: Wireshark 1.6.7.

b. Hardware

- Wireless Access Points: Cisco-Linksys Wireless-G Broadband Router (model WRT54GL) and ASUS Black Diamond Dual-Band Wireless-N 600 Router (RT-N56U)
- Cisco router 2600
- Three Laptops (HP Pavilion dv6, Lenovo ThinkPad T510 and DELL Latitude D830).

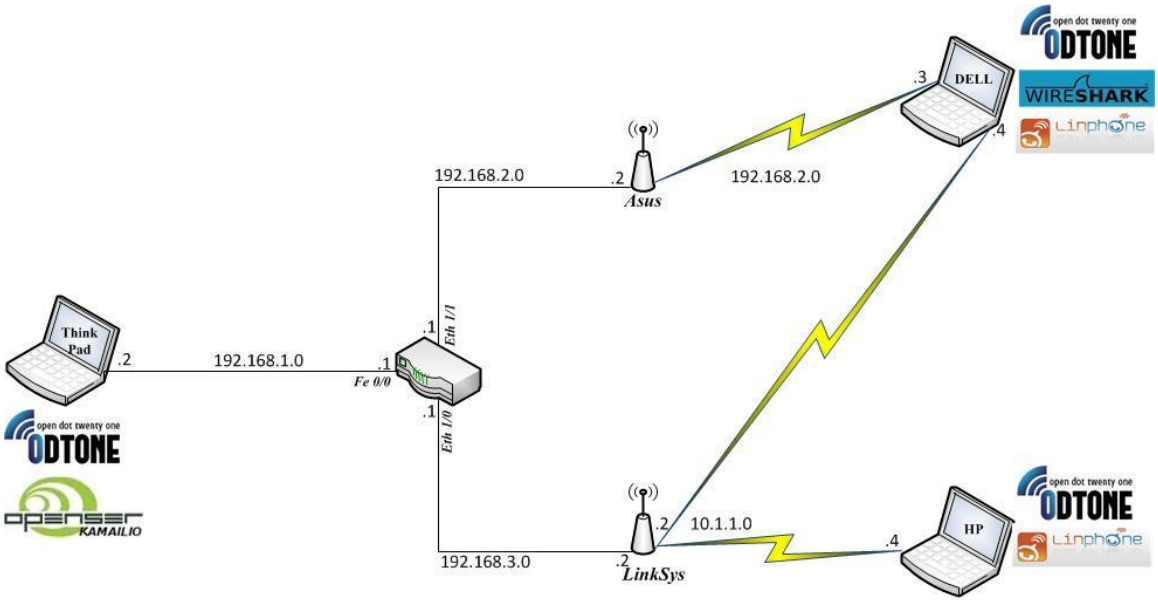

Figure 14. Test Bed

Figure 14 illustrates the test bed used during the tests and shows the configuration of software and hardware and the IP address of each node in the network.

2. Test 1: Using Two NICs for the Mobile Node

We tried first to equip the MH with two wireless network cards: the first connected to the home network (HN) and the second connected to the foreign network

(FN). The results were unsatisfactory, because none of the UA aforementioned could maintain the multimedia session after disconnecting the card connected to the HN in order to move the UA to the FN. One problem was that some UA (e.g., in the case of Linphone) is configured to use only one network card, and would crash or stop the conversation after that card was disconnected. Thus, we decided to use only one network card and move the MN (physically) between networks (HN and FN), or disconnect from one and instantaneously connect to the other.

3. Test 2: Using One NIC for the Mobile Node

During this experiment, we tried to test different user agents because not all of them are compliant to RFC 3261 or RFC 6141. We did know a priori which UA supports the mid-call mobility while conserving an acceptable quality of service (video and sound quality). In order to decide which is best, we performed a comparison between the different UAs mentioned before. Table 1 shows the result of this comparison:

UA	OS	Support mobility or not	Observations
Ekiga 3.3.2	Linux	NO	Had problems even for regular calls
Jitsi 1.0	Linux/Windows	NO	Detected the address change and stopped sending media data. Didn't crash and continued the session when the MH moved back to the HN.
Linphone 3.3.2	Linux/Windows/iOS	NO	Maintained the media session. Needs better investigation and tests.
Windows Messenger 5.0	Windows	NO	Had problems starting a conversation; needed specific configuration parameters with Kamailio
X-lite	Windows (not available on Linux)	NO	

Table 1. Test Results

F. INTEGRATION OF ODTONE AND SIP (LINPHONE)

Test 2 (Experiment 2) demonstrated that linphone is the best SIP client so we decided to use it for testing the integration of MIH and SIP in order to provide seamless mobility. The developers of Linphone claim that it conforms to RFC 3261, but when we tried to move from a network to another to trigger a re-INVITE message, we didn't see that the MH sent a re-INVITE message. The CH didn't get the new MH's IP and stopped the communication.

A workaround to this problem is to develop a separate software program that subscribes to the ODTONE MIES function and sends a re-INVITE message on behalf of the mobile node when the mobile node is about to switch to a new network. To do so, we went through three iterations of software development, which are detailed below.

We used the same software platform (Figure 14) as in the previous experiments: Linphone as SIP client, Kamailio as SIP server, and Wireshark for network sniffing. Furthermore, we used Nemesis for crafting packets carrying the required SIP re-INVITE messages.

1. Experiment 1: Malformed Packets

During this stage, we tried to use the script to send an INVITE packet from the mobile node to the SIP server; however, the server didn't forward the and considered it a malformed packet.

After some investigation, we found that the packet we created had the wrong payload (the SIP message). In order to get a valid SIP message that could be accepted and then forwarded by the server, we started a communication between the SIP clients and sniffed the packets exchanged during the connection establishment using Wireshark. Then we copied the SIP message content into a file as input to Nemesis (Figure 15), using the following Nemesis command:

nemesis udp –v –S *192.168.2.3* –D *10.1.1.100* –x *5060* –y *5060* –P *sip_payload1*

```
OETK$%&AD\|BINVITE sip:mih-dell@192.168.2.3 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.100:5060;rport;branch=z9hG4bK95301
From: <sip:mih-hp@192.168.1.2>;tag=88769
To: "mih-dell" <sip:mih-dell@192.168.2.3>
Call-ID: 30127
CSeq: 20 INVITE
Contact: <sip:mih-hp@10.1.1.100>
Content-Type: application/sdp
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Max-Forwards: 70
User-Agent: Linphone/3.5.2 (eXosip2/3.6.0)
Subject: Phone call
Content-Length: 631

v=0
o=mih-dell 123456 654321 IN IP4 10.1.1.100
s=A conversation
c=IN IP4 10.1.1.100
t=0 0
m=audio 7078 RTP/AVP 112 111 110 3 0 8 101
a=rtpmap:112 speex/32000/1
a=fmtp:112 vbr=on
a=rtpmap:111 speex/16000/1
a=fmtp:111 vbr=on
a=rtpmap:110 speex/8000/1
a=fmtp:110 vbr=on
a=rtpmap:3 GSM/8000/1
a=rtpmap:0 PCMU/8000/1
a=rtpmap:8 PCMA/8000/1
a=rtpmap:101 telephone-event/8000/1
a=fmtp:101 0-11
m=video 9078 RTP/AVP 99 97 98 34 100
a=rtpmap:99 MP4V-ES/90000
a=fmtp:99 profile-level-id=3
a=rtpmap:97 theora/90000
a=rtpmap:98 H263-1998/90000
```

Figure 15. SIP Message : *sip_payload1*

We then tried to replay the same packet after tearing down the ongoing communication. Again, the server didn't forward the re-message and blocked it as shown in the Wireshark screen capture in Figure 16.

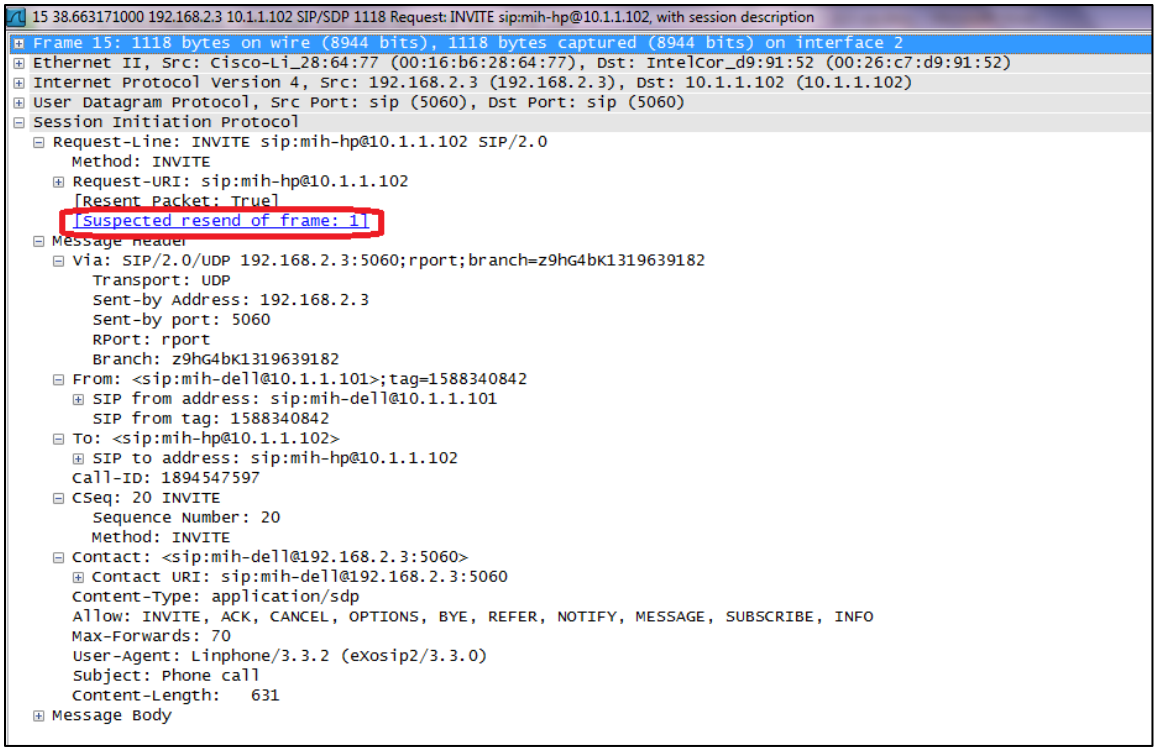

Figure 16. SIP Message Replay Detection

2. Experiment 2: Parameters Problem (Brunch and Tag)

During this experiment, we used the same payload file sniffed previously, but we changed the brunch, call-ID, and the tag, as displayed in Figure 17, to make the message unique and to avoid the replay detection.

RFC 3261 defines the parameters that need to be changed during a call:

- Call-ID: A unique identifier of the call (RFC 3261)
- Branch: A unique identifier of the INVITE message and should start with the characters "z9hG4bK" (RFC 3261)
- Tag: Used in the “To” and “From” fields to identify a dialog, it should be a randomly generated number (RFC 3261)

```
INVITE sip:mih-dell@192.168.2.3 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.102:5060;rport;branch=z9hG4bK3940
From: <sip:mih-hp@192.168.1.2>;tag=19830
To: "mih-dell" <sip:mih-dell@192.168.2.3>
Call-ID: 4396
CSeq: 20 INVITE
Contact: <sip:mih-hp@10.1.1.102>
Content-Type: application/sdp
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Max-Forwards: 70
User-Agent: Linphone/3.5.2 (eXosip2/3.6.0)
Subject: Phone call
Content-Length:   475

v=0
o=mih-hp 2672 2672 IN IP4 10.1.1.102
s=Talk
c=IN IP4 10.1.1.102
t=0 0
m=audio 7078 RTP/AVP 112 111 110 3 0 8 101
a=rtpmap:112 speex/32000
a=fmtp:112 vbr=on
a=rtpmap:111 speex/16000
a=fmtp:111 vbr=on
a=rtpmap:110 speex/8000
a=fmtp:110 vbr=on
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
m=video 9078 RTP/AVP 103 99 98
a=rtpmap:103 VP8/90000
a=rtpmap:99 MP4V-ES/90000
a=fmtp:99 profile-level-id=3
a=rtpmap:98 H263-1998/90000
a=fmtp:98 CIF=1;QCIF=1
```

Figure 17. SIP Message Experiment 2

After making these changes, we were still unable to make the server forward the INVITE message to the desired SIP client. This time, the error was the size of the payload file.

After reviewing some published SIP-based attacks such as SIP re-attack, SIP spoof, and SIP denial of service attacks we found a code example that generates a fake message (Figure 18) that may trick a SIP client. We revised our program based on this example for the next experiment.

```
1  INVITE sip:mih-dell@192.168.2.3 SIP/2.0
2  Via: SIP/2.0/UDP 10.1.1.102:5060;rport;branch=z9hG4bK3840
3  From: <sip:mih-hp@192.168.1.2>;tag=19840
4  To: "mih-dell" <sip:mih-dell@192.168.2.3>
5  Call-ID: 4386
6  CSeq: 20 INVITE
7  Contact: <sip:mih-hp@10.1.1.102>
8  Content-Type: application/sdp
9  Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
10 Max-Forwards: 70
11 User-Agent: Linphone/3.5.2 (eXosip2/3.6.0)
12 Subject: Phone call
```

Figure 18. Successful SIP Message

3. Experiment 3: All parameters Fixed According to RFC3665

After being able to craft a "legitimate" message we consulted RFC 3665, which describes the flow of the re-(Figure 19) message used to inform the correspondent node that the MN has changed its IP address.

RFC 3665 describes the message flow and all the parameters that need to be changed. In particular, an example scenario is provided in Section 3.7 of the RFC, which describes a session where the mobile node moves to the foreign network and informs the correspondent node of its new IP address using a SIP re-INVITE message.

```
F9 INVITE Bob -> Alice

INVITE sip:alice@client.atlanta.example.com SIP/2.0
Via: SIP/2.0/UDP client.chicago.example.com:5060;branch=z9hG4bKlkld5l
Max-Forwards: 70
From: Bob <sip:bob@biloxi.example.com>;tag=314159
To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
CSeq: 14 INVITE
Contact: <sip:bob@client.chicago.example.com>
Content-Type: application/sdp
Content-Length: 149

v=0
o=bob 2890844527 2890844528 IN IP4 client.chicago.example.com
s=-
c=IN IP4 192.0.2.100
t=0 0
m=audio 47172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

Figure 19. SIP Re-Message with IP Change (RFC 3665)

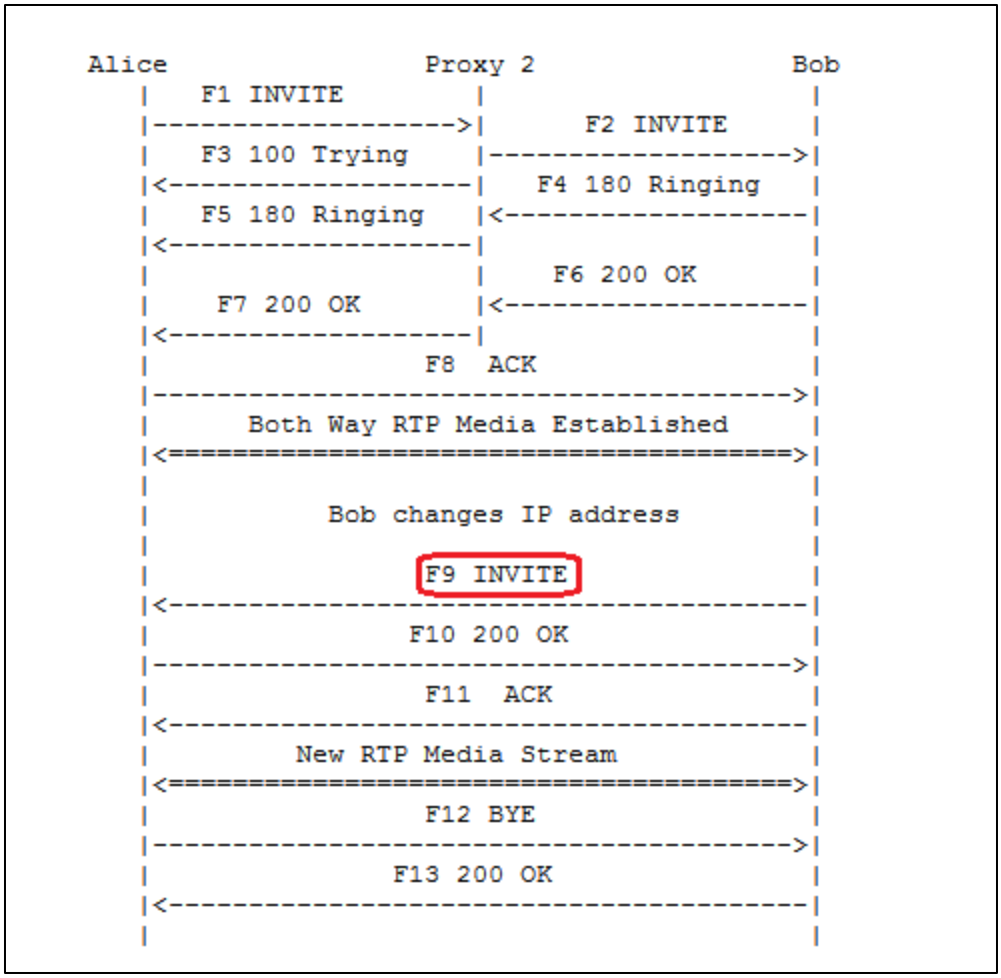

Figure 20. Session with Re-INVITE (RFC 3665)

We started a "legitimate" communication between the two SIP clients and then sniffed the SIP messages exchanged between the two nodes in order to use the right parameters to generate a SIP re-message. We were able to generate a message using the following payload file and the following command:

nemesis udp –v –S *192.168.2.3* –D *10.1.1.100* –x *5060* –y *5060* –P *sip_payload1* -FD –I *0* –T *64*

Figure 21 shows the crafted message; it shows the parameters that have been changed in order to make a valid re-message.

```
1  INVITE sip:mih-dell@192.168.2.3 SIP/2.0
2  Via: SIP/2.0/UDP 10.1.1.100:5060;rport;branch=z9hG4bK13523
3  From: <sip:mih-hp@192.168.1.2>;tag=28778
4  To: "mih-dell" <sip:mih-dell@192.168.2.3>;tag=29728
5  Call-ID: 31985
6  CSeq: 24 INVITE
7  Contact: <sip:mih-hp@10.1.1.100>
8  Content-Type: application/sdp
9  Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
10 Max-Forwards: 70
11 User-Agent: Linphone/3.5.2 (eXosip2/3.6.0)
12 Subject: Phone call
13
14 v=0
15 o=mih-dell 123456 654321 IN IP4 192.168.2.3
16 s=A conversation
17 c=IN IP4 192.168.2.4
18 t=0 0
19 m=audio 7078 RTP/AVP 112 111 110 3 0 8 101
20 a=rtpmap:112 speex/32000/1
21 a=fmtp:112 vbr=on
22 a=rtpmap:111 speex/16000/1
23 a=fmtp:111 vbr=on
24 a=rtpmap:110 speex/8000/1
25 a=fmtp:110 vbr=on
26 a=rtpmap:3 GSM/8000/1
27 a=rtpmap:0 PCMU/8000/1
28 a=rtpmap:8 PCMA/8000/1
29 a=rtpmap:101 telephone-event/8000/1
30 a=fmtp:101 0-11
31 m=video 9078 RTP/AVP 99 97 98 34 100
32 a=rtpmap:99 MP4V-ES/90000
33 a=fmtp:99 profile-level-id=3
34 a=rtpmap:97 theora/90000
35 a=rtpmap:98 H263-1998/90000
36 a=fmtp:98 CIF=1;QCIF=1
```

Figure 21. Valid SIP Re-INVITE message

Unfortunately, Linphone didn't accept the message. Figure 22 shows how the Linphone program reacted to the re-INVITE message. In the 30 to 60s after receiving the message, the program crashed and stopped communication (Figure 22).

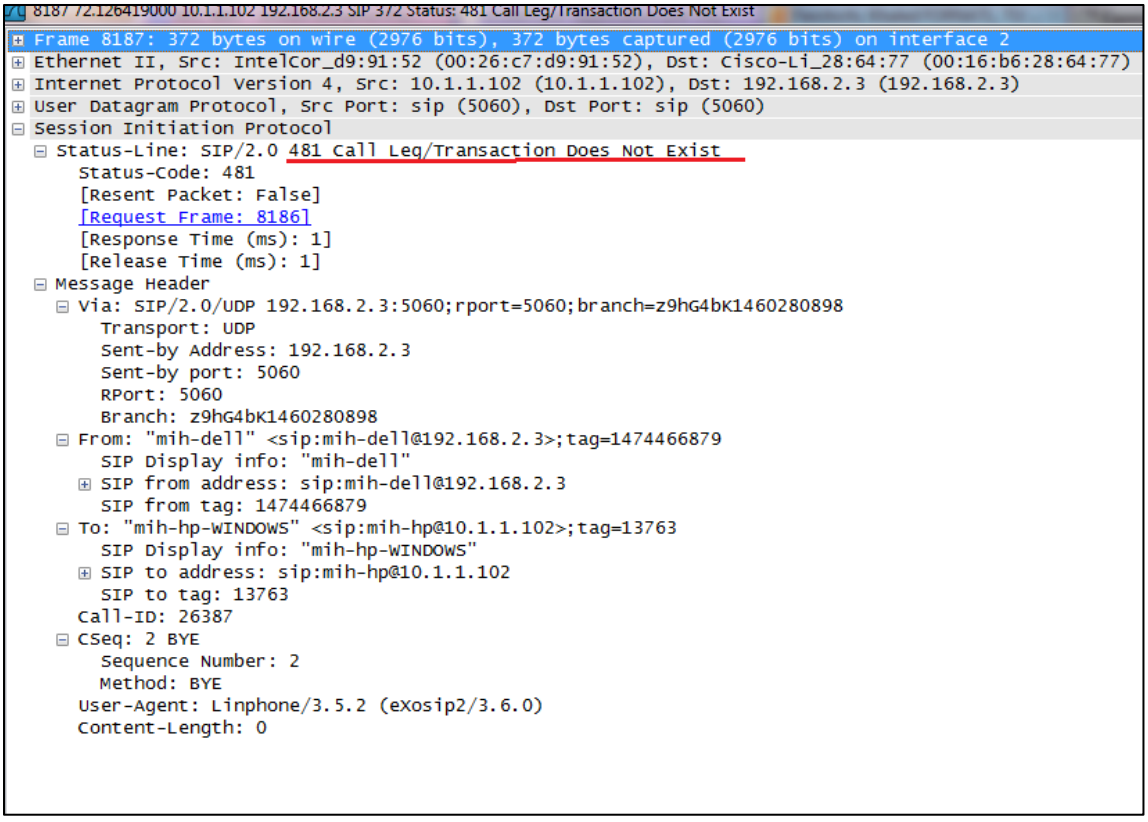

Figure 22. Re-INVITE Message Not Accepted

G. CHAPTER CONCLUSION

The SIP clients that we tried didn't fully support the re-INVITE message, even though it was defined in the RFC 3261. The re-message without proper security safeguards such as encryption and authentication can be a strong attack vector that can be exploited by hackers to hijack calls or tear down a communication by modifying its parameters (audio, video, IP address, etc.). For this reason, the functionality was omitted by most SIP UA developers.

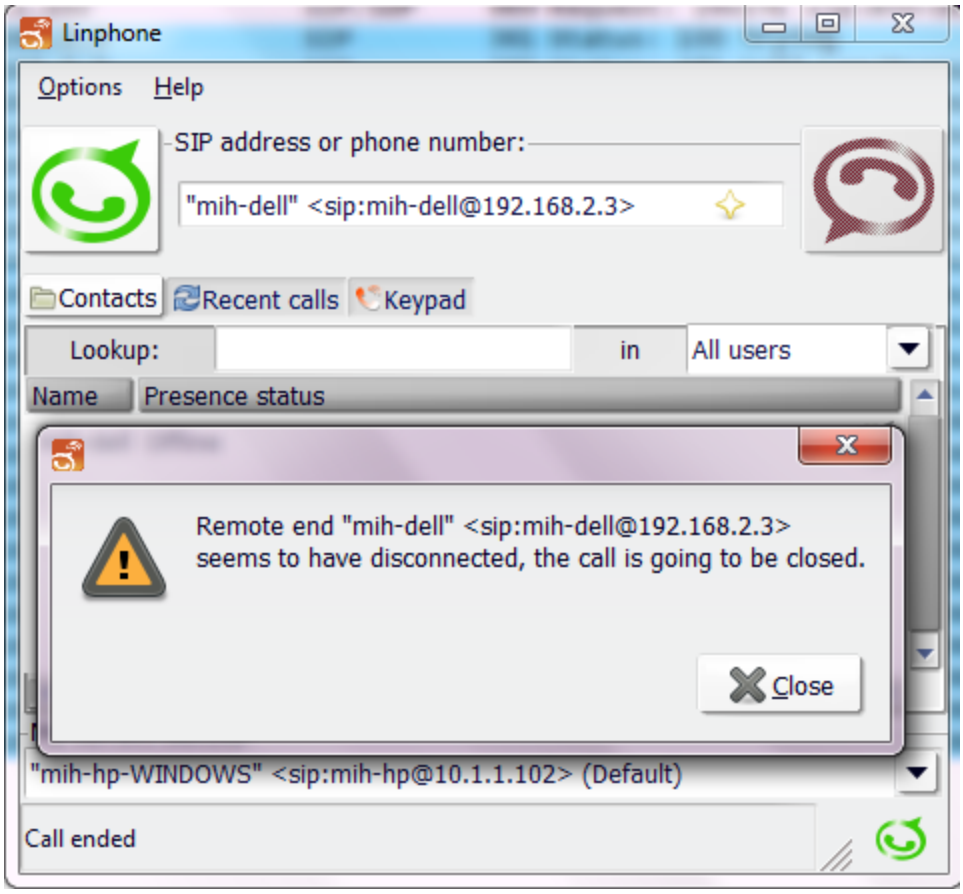

Figure 23. Linphone Crash after Re-INVITE Message

V. CONCLUSIONS AND FUTURE WORK

A. CONCLUSION

The installation and test of the ODTONE framework was beneficial because it showed the advantages that MIH can provide. In fact, IEEE 802.21 is an ambitious protocol that can be very useful to users if deployed in large scale by carriers.

During tests and experimentation, the researchers wanted to demonstrate how beneficial this technology can be if integrated into HFNs. To do so, we created a test bed that mimics in a small scale their architecture. The installation and deployment of ODTONE was successful, based on the previous research done by another NPS student (Ohleger, 2012). Then we decided to test ODTONE with SIP in order to provide HFN users and first responders with seamless mobility in the conversation space.

There are many standards that address mobility issues. Given that MIH provides Layer 2 information for seamless handover, we had to choose another protocol that would trigger the handover. We choose SIP for application mobility, because it was easier to implement and test. Other protocols such as MIP, MIPv6, PMIPv6, etc. needed specific hardware to be implemented (some version of Cisco routers). MIH and SIP can provide the perfect solution for mobility, because we are taking advantage of Layer 2 information to trigger handovers on the application layer.

None of the SIP UA that we tested implemented SIP application-layer mobility, however we were able to see the huge benefits that ODTONE can provide if integrated with a SIP UA. The main reason UA developers avoided the implementation of SIP application-layer mobility was security risks. Actually, SIP application-layer mobility is an attack vector that can be easily exploited by hackers.

During our tests we noticed, also, that MIH does not provide any security mechanisms for the network nodes or servers. All the messages are sent in the clear; there is neither encryption nor authentication. An attacker can easily spoof IPs and start sending advertisements and messages that can drastically alter the behavior of the network nodes. He can make them switch from network to another network, make a

network unavailable by sending “link up”/”link down” messages, hijack sessions, or even shut down network interfaces. The MIH standard doesn’t address security issues and leaves it to other layers of protocol, which make it less attractive to the industry.

Our research showed the advantages and benefits of MIH/ODTONE and the steps needed to implement and integrate a mobility solution based on SIP and MIH. Such a solution is not only valid in the HFN context but can be useful in any military or civilian environment.

B. FUTURE WORK

In this section, we will provide ideas of future research dealing with both MIH and SIP.

First, the IEEE 802.21 is still not fully exploited and not yet largely implemented by the industry. This research was beneficial in understanding how it can be fully integrated with existing mature technologies such as SIP. The integration should be done in two phases (we will take Linphone as UA example):

- First, the modification of Linphone (open source) to support the capability of subscription and reading of events from ODTONE MIES in order to get layer-two information messages such as “link up,” “link down,” “link going down,” etc.
- Second, the modification of Linphone code source to support and implement application layer mobility as defined by RFC 3261. Precisely make changes to Linphone in order to support the re-invite message and trigger an IP change when the connection is going down or when it founds (Through MIES) that there is a better network available.

Second, IEEE 802.21 security needs to be investigated in depth before any implementation attempt. The protocol designers left the security to other layers, which can be a huge problem during real deployment of the protocol. It has also some noticeable attack vectors, such as the absence of encryption and the absence of authentication, especially for MIIS servers.

LIST OF REFERENCES

Cacace, F., & Vollero, L. (2006). Managing mobility and adaptation in upcoming 802.21 enabled devices. *Proceedings of the 4th international workshop on wireless mobile applications and services on WLAN hotspots – WMASH '06*, 1–10. doi:10.1145/1161023.1161025

Carlos, G., & Bruno, S. (2012). *ODTONE 0.4.* Retrieved from http://atnog.av.it.pt/odtone/documentation.html

Corujo, D., Guimaraes, C., Santos, B., & Aguiar, R. L. (2011). Using an open-source IEEE 802.21 implementation for network-based localized mobility management. *Communications Magazine*, IEEE, *49*(9), 114–123.

Cicconetti, C. , Galeassi, F. , Mambrini, R. (2011). A Software Architecture for Network-Assisted Handover in IEEE 802.21. *Journal of Communications*, *6*(1), 44–55, doi:10.4304/jcm.6.1.44–55

De La Oliva, A., Banchs, A., Soto, I., Melia, T., & Vidal, A. (2008). An overview of IEEE 802.21: Media-independent handover services. *Wireless Communications, IEEE*, *15*(4), 96–103.

Denning, P. J. (2006). Hastily formed networks. *Communications of the ACM*, *49*(4), 15. doi:10.1145/1121949.1121966

Eastwood, L., Migaldi, S., Qiaobing Xie, & Gupta, V. (2008). Mobility using IEEE 802.21 in a heterogeneous IEEE 802.16/802.11-based, IMT-advanced (4G) network. *Wireless Communications*, IEEE, *15*(2), 26–34.

Hastily formed networks for complex humanitarian disasters. (2012, July 7) Retrieved from http://www.docstoc.com/docs/79936215/HASTILY-FORMED-NETWORKS-FOR-COMPLEX-HUMANITARIAN-DISASTERS

Schulzrinne, H. and Wedlund, E. (2000). Application-layer mobility using SIP. *ACM SIGMOBILE Mobile Computing and Communications*, *4*(3), 47–57. doi:10.1145/372346.372369

Lim, W., Kim, D., Suh, Y., & Won, J. (2009). Implementation and performance study of IEEE 802.21 in integrated IEEE 802.11/802.16e networks. *Computer Communications*, *32*(1), 134–143. doi:10.1016/j.comcom.2008.09.034

Lopez, Y., & Robert. OpenMIH, an open-source media-independent handover implementation and its application to proactive pre-authentication. *Mobile Networks and Management*, 32, 14–25. doi: 10.1007/978-3–642-11817-3_2

Ohleger Jr., M. P. (2012). Media Independent handover for wireless full motion video dissemination (Master's thesis). Naval Postgraduate School. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a567262.pdf

Module 8: Overview of SIP (2012, November 19) Retrieved from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CDMQFjAA&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2Fc%2Fd%2Ff%2Fcdf3c55a-fc5b-46ae-9030–44e44935f003%2F2081a_08.pdf&ei=FCarUM-ODeHvigLb94DwDA&usg=AFQjCNGmtAt91cdmacES-5P79Aj5aWMR3g&sig2=iKDJ7xScgmKerXhDcEgxcA

Mohamad, S. (2008). *Modélisation et simulation des réseaux mobiles de 4ème génération.* Retrieved from: http://www.tesa.prd.fr/docs/journalTESA /These_Mohamad_Salhani.pdf

Muhammad, M., Rehan. (2009). Investigation of IEEE 802.21 'Media Independent Handover' service suitability for TCP based flows in heterogeneous mobile environment (Master's thesis). Mohammad Ali Jinnah University:Pakistan. Retrieved from http://www.academia.edu/574529/investigation_of_ieee _802.21_media_independent_handoverservice_suitabilty_for_tcp_based_flows_in_heterogeneous_mobile_

Mussabbir, Q. B., & Yao, W. (2006). Optimized FMIPv6 handover using IEEE802.21 MIH services. *MobiArch06 First International Workshop on Mobility in the Evolving Internet Architecture*, 43. doi:10.1145/1186699.1186713

Nakajima, N., Dutta, A., Das, S., & Schulzrinne, H. (2003). Handoff delay analysis and measurement for SIP based mobility in IPv6. *Communications, 2003. ICC '03. IEEE International Conference on*, *2*(2), 1085–1089.

Nelson, C. B., Steckler, B. D., & Stamberger, J. A. (2011). The evolution of hastily formed networks for disaster response: Technologies, case studies, and future trends. *IEEE global humanitarian technology conference*, 467–475. doi: 10.1109/GHTC.2011.98

Piri, E., & Pentikousis, K. (2009). Towards a GNU/Linux IEEE 802.21 implementation. *Communications, 2009. ICC '09. IEEE International Conference*, 1–5. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5199534&tag=1

Silva, R., Carvalho, P., Sousa, P., & Neves, P. (2011; 2011). Enabling heterogeneous mobility in android devices. *Mobile Networks and Applications*, *16*(4), 518–528. doi:10.1007/s11036–011–0322–6

SIP Tutorials. (2009, November 19). Retrieved from http://www.siptutorial.net/SIP/index.html

SIP: Session initiation protocol. (2002). Retrieved November 19, 2012, from http://www.ietf.org/rfc/rfc3261.txt

Steckler, B. D. (2012, September 18). *HFN nine-element puzzle*. Retrieved from http://faculty.nps.edu/dl/HFN/puzzle_piece/puzzle_piece.htm

*Survey of IEEE802.21 MIH. (*2012, July 3). Retrieved from http://www.cse.wustl.edu/~jain/cse574–06/ftp/handover/index.html

Taniuchi, K., Ohba, Y., Fajardo, V., Das, S., Tauil, M., Yuu-Heng Cheng, & Famolari, D. (2009). IEEE 802.21: Media independent handover: Features, applicability, and realization. *Communications Magazine*, IEEE, *47*(1), 112–120. Retrieved from ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4752687

Yeh, C-H, Wu, Q, & Lin, Y-B. (2006). SIP terminal mobility for both IPv4 and IPv6. *ICDCSW '06 Proceedings of the 26th IEEE International Conference Workshops on Distributed Computing Systems*, 53–53. doi:10.1109/ICDCSW.2006.99

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Geoffrey Xie
   Naval Postgraduate School
   Monterey, California

4. Brian Steckler
   Naval Postgraduate School
   Monterey, California

5. Dan Boger
   Naval Postgraduate School
   Monterey, California